USER MANUAL

All Appliance Models

Software Release 3.2

By:

Table of Contents

Preface: About This Manual 7

1 WiDirect Administration Interface 8

1.1 Logging In 8

1.2 System Status Menu 8

1.2.1 Home 8
1.2.2 Active Users 8
1.2.3 Event Viewer 9
1.2.4 AP Status 10
1.2.5 Bridge Status 12
1.2.6 Access Point Map Display 12
1.2.7 System Check 13

1.3 Users Menu 14

1.3.1 Viewing All Users (List All) 14
1.3.2 Find User 16
1.3.3 Add User 17
1.3.4 Banning MAC Addresses 17
1.3.5 Viewing User Details 18
1.3.6 View User's Connection History 19

1.4 User Experience Menu 19

1.4.1 Preferences 19
1.4.2 Walled Garden 24
1.4.3 Blocked Sites 24
1.4.4 Message of the Day 25
1.4.5 Profile Branding 25
1.4.6 Radius 29

1.5 Social Networking 30

1.5.1 Overview 30
1.5.2 Facebook 30
1.5.3 Google+ 32
1.5.4 LinkedIn 34

1.6 Reports 36

1.6.1 Functionality Overview 36
1.6.2 Connections 36
1.6.3 Registrations 36
1.6.4 Purchases 36
1.6.5 Overall Usage 36
1.6.6 Billing (Purchases) 37
1.6.7 Access Point Usage 37
1.6.8 Downloads 37

1.7 System Configuration 38

1.7.1 Profiles 38
1.7.2 Access Plans 38
1.7.3 Coupons 41
1.7.4 Voucher Admin 41
1.7.5 Access Points 41

1.7.6 WiClients and WCMS 43
1.7.7 Payment Gateways 44
1.7.8 Network Configuration 47
1.7.9 Network Routing 48
1.7.10 Date and Time 48
1.7.11 Log Viewer 49
1.7.12 License Key 49
1.7.13 Admin Users 50
1.7.14 SmartEdge 52
1.7.15 UAM 52
1.7.16 Shutdown 52
1.7.17 Support 53
1.8 Services Menu 54
1.8.1 DHCP 54
1.8.2 Radius 55
1.8.3 HTTP 55
1.8.4 Firewall 56
1.8.5 NTP 61
1.8.6 Preproxy 62
1.8.7 Web Cache 62
1.8.8 DNS 62
1.9 Access Point Support 64
1.9.1 Ericsson 64
1.9.1.1 Access Point Configuration 64
1.10 Tools 65
1.10.1 Ping 65
1.10.2 Traceroute 65
1.10.3 DNS Query 65
1.11 Voucher Management Page 66
1.11.1 Create Single Guest-Pass 66
1.11.2 Create Batch Guest-Pass 67
1.11.3 List 68
1.11.4 Search 68
1.11.5 Delete Vouchers 69
2 Command Line Interface 70
2.1 Secure Shell access 70
2.2 Using sudo commands 70
2.3 Changing the password 70
2.4 Restarting System Services 71
2.5 Restart Watchdog Process 71
2.6 Generate SSL Key and Certificate 71
2.7 Using Emacs to Edit Files 72
2.8 Configure Port Forwarding 72
2.9 Using Tcpdump to Monitor Traffic 72

2.10 Using Arping to Test a User's Connection 73
2.11 Access SQL database 73
2.11.1 Reset failed login attempts 73
2.11.2 Recover GUI Administrator Password 73
2.12 More Information 73
3 Installation ***74***
3.1 Support Services 74
3.2 Example Network Diagram 74
3.2.1 Basic Setup and Configuration 75
3.2.2 Acceptance Testing of Sample Network 83
4 Special Deployment Scenarios ***84***
4.1 Enabling MAC Authentication for Specific Stations 84
4.2 Customizing a Network by Profile 84
4.2.1 Configure the Profiles 84
4.2.2 Branding 85
4.2.3 Access Plans 85
4.3 Configuring VLANs 85
4.3.1 Create VLAN 85
4.3.2 Configure DNS and DHCP Servers 85
4.3.3 Configure Firewall 85
4.4 Setup Recurring Billing with Authorize.net CIM 86
4.4.1 Payment Gateways 86
4.4.2 Access Plans 86
4.4.3 User Details 86
4.4.4 Email Templates 86
4.4.5 Failed Payments 86
4.4.6 Activating Accounts 86
4.4.7 Making a Payment 86
4.4.8 Update Account 87
4.5 Turning off External DNS Resolution 87
4.6 Hiding Access Plans from Users 87
4.7 Entering Ingress (From Internet) Firewall Rules 88
4.8 Disabling DHCP Dependency 88
4.9 Disabling NAT (Network Address Translation) 89

4.10 Enable Ping on WAN Interface 89
4.11 How to Disable Mobile Node Access to the Admin Pages 90
4.12 Login and Logout URL 90
4.13 Sendmail SMTP Configurations 91
4.13.1 Updating the SMTP domain name 91
4.13.2 Adding an SMTP Relay 91
4.13.3 Restarting the Sendmail Process 91
4.14 Hosted WiDirect 92
4.15 Disable Proceed Page When Using MAC Authentication 92
4.16 Automatically Logout Dead Connections 92
4.17 Increased Customization of Login Page 92
4.18 Enable SNMP Monitoring of the WiDirect 93
4.19 Automatic Login on Multiple Devices 94
4.20 Throttle Bandwidth after Limit Reached 94
4.21 Configure SmartEdge Authentication 95
4.21.1 Modify configuration files 95
4.21.2 Modify GUI Settings 95
4.22 Configure UAM 95
4.23 Performing a System Backup 96
4.24 Performing a System Recovery 97
4.25 Modify Custom Configuration Settings 98
5 Administration & Maintenance ***100***
5.1 Active Users 100
5.2 Event Viewer 100
5.3 AP Status and Transit Link Graph 100
5.4 System Check 100
5.5 System Verification 100
5.5.1 Verify Processes 100
5.5.2 Verify Captive Portal Features 100
5.5.3 Speed Testing 101
5.5.4 Ping Test 101
5.5.5 DNS Verification 101
5.5.6 Verify APs 102
6 Software ***103***
6.1 Software Upgrades & Patching 103
6.2 Logs and Log Rotation 103
6.3 Log Location 103

7 Hardware Diagrams _____ *104*

*8 Technical Support*_____ *108*

The information in this User Manual has been carefully reviewed and is believed to be accurate. AllCity Wireless assumes no responsibility for any inaccuracies that may be contained in this document, makes no commitment to update or to keep current the information in this manual, or to notify any person or organization of the updates. For the most up-to-date version of this manual, please visit the AllCity Wireless support website at http://www.allcitywireless.com/support/. AllCity Wireless reserves the right to make changes to the product described in this manual at any time and without notice. This product, including software, if any, and documentation may not, in whole or in part, be copied, photocopied, reproduced, translated or reduced to any medium without prior written consent.

IN NO EVENT WILL ALLCITY WIRELESS, LLC. BE LIABLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING FROM THE USE OR INABILITY TO USE THIS PRODUCT OR DOCUMENTATION, EVEN IF ADVISED OF THE POSSIBILITY OR SUCH DAMAGES. IN PARTICULAR, ALLCITY WIRELESS, LLC. SHALL NOT HAVE LIABILITY FOR ANY HARDWARE, SOFTWARE, OR DATA STORED OR USED WITH THE PRODUCT, INCLUDING THE COSTS OF REPAIRING, REPLACING, INTEGRATING, INSTALLING OR RECOVERING SUCH HARDWARE, SOFTWARE, OR DATA.

Any disputes arising between manufacturer and customer shall be governed by the laws of Anne Arundel County in the State of Maryland, USA. The State of Maryland shall be the exclusive venue for the resolution of any such disputes. AllCity Wireless' total liability for all claims will not exceed the price paid for the hardware product. Unless you request and receive written permission from AllCity Wireless, you may not copy any part of this document. Information in this document is subject to change without notice. Other products and companies referred to herein are trademarks or registered trademarks of their respective companies or mark holders.

Copyright 2014 by AllCity Wireless, LLC.
All rights reserved.
Printed in the United States of America

Revision History

Rev	Date	Editor	Description
3.0	2/12/13	DV	Updated for version 3.0
3.2	8/29/14	DV	Updated for version 3.2

Preface: About This Manual

This manual is written for system administrators, system integrators, network administrators and others who use the WiDirect appliance. The WiDirect models span a broad spectrum of possible applications. The product can be used to manage wire line and wireless networks, both local and remote. The WiDirect gives the ability to segment the network into multiple profiles, and to provide a unique user experience based on the user's location.

The WiDirect line is split into two classifications, Authentication Server and Client. All networks initially require a WiDirect Authentication Server which has the ability to function independently. Through WiDirect Client Management Service (WCMS), WiClients can be added to expand the network size, both from local user processing and to expand in different geographic locations. The smaller models are appropriate for small office applications and local WISP applications. Larger models can manage common carrier network environments. Each WiDirect unit contains the same software and most of the features are available for use in each model. The most notable differences pertain to embedded firmware and Micro model line. The feature set within the WiDirect appliance is broad and is expected to continue to grow over time. These features provide significant capabilities that create a network infrastructure, one that can be used in numerous creative ways depending on the environment.

If you are installing a WiDirect for the first time, you should read this entire manual in order to become familiar with the settings and tools. However, the steps to actually install and configure a new WiDirect box begin with *Section 3: Installation.* Other helpful answers to common questions can be found in *Section 4: Special Deployment Scenarios*.

1 WiDirect Administration Interface

1.1 Logging In

In order to gain initial access to the WiDirect's web based GUI, a cross-over cable can be connected between the Eth1 (Ethernet 1) interface and another computer. See *Section 7: Hardware Diagrams* for a diagram of the Ethernet ports. The WiDirect will provide the other machine with an IP address in the 10.4.1.0/24 subnet via DHCP. (Be sure that the connecting computer is configured for DHCP to receive the IP address.)

Once the IP address has been established, open a web browser such as Firefox, and open the following URL:

http://10.4.1.1/portal/admin

This URL opens the WiDirect Admin login page. To login, use the default username ***admin*** and the password ***widirect***.

Note: If the IP address of Eth1 has changed from the default, use the new IP address instead of 10.4.1.1.

WARNING: For security reasons, if a user fails to enter the proper login credentials five times in a row, their IP address will be banned from the login page for fifteen minutes. After fifteen minutes have passed, they'll be able to attempt another login.

1.2 System Status Menu

The system status menu is the first menu that is located in the left hand navigation bar of the WiDirect web GUI.

1.2.1 Home

The ***Home*** button, which is located in the top left hand corner of the administrator page, returns the user to the home screen. This is the same page that is displayed upon first logging into the WiDirect. The home page gives a quick status on the number of users that are currently connected to the WiDirect.

1.2.2 Active Users

The *Active Users* page as shown in Figure 1-1 displays all the information about users that are currently connected to the WiDirect.

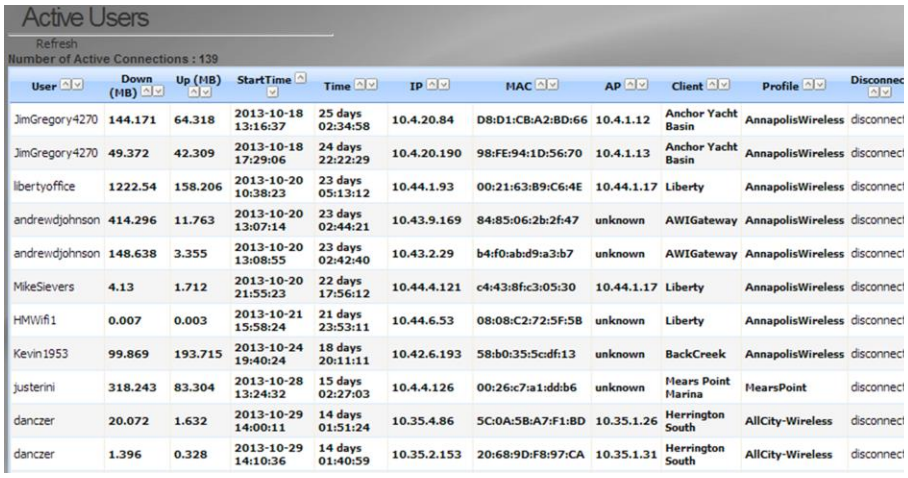
The table provides the username, traffic, start time, time connected, IP, MAC, Access Point (AP), Client, and Profile. See Table 1-1 for more information on each entry.

Field	**Description**
User	The username of the user connected to the WiDirect. Clicking this links brings up the user details page for that user.
InBytes & OutBytes	The amount of bandwidth (in bytes) the user has used for this session.
Start Time	The date and time the session began.
Time	Total time connected for this session in Hours: Minutes: Seconds.
IP	The IP address the user is currently using. If the network has multiple WiClients using the same subnet, then users may appear to be using the same IP address.
MAC	The user's current MAC address.

AP	The AP the user is on. Only available if the *getapfromradius* is enabled in the firewall. The AP will be determined either from RADIUS messages or from DHCP relay requests. See Firewall configuration for more information. Otherwise, the AP will display as "unknown."
Client	The client that the user is currently connected to.
Profile	The profile the user has associated with for this session. Profiles are used to provide a custom user experience depending on where the user is located.
Disconnect	Clicking on this link will automatically disconnect the user from the network.

Table 1-1: Active User Fields

The ***Disconnect*** button at the end of each row allows administrators to quickly disconnect individual users. There is a ***Disconnect All*** button at the bottom of the page that allows an administrator to completely disconnect all active users in a single step.



User	Down (MB)	Up (MB)	StartTime	Time	IP	MAC	AP	Client	Profile	Disconnec
JimGregory4270	144.171	64.318	2013-10-18 13:16:37	25 days 02:34:58	10.4.20.84	D8:D1:CB:A2:BD:66	10.4.1.12	Anchor Yacht Basin	AnnapolisWireless	disconnect
JimGregory4270	49.372	42.309	2013-10-18 17:29:06	24 days 22:22:29	10.4.20.190	98:FE:94:1D:56:70	10.4.1.13	Anchor Yacht Basin	AnnapolisWireless	disconnect
libertyoffice	1222.54	158.206	2013-10-20 10:38:23	23 days 05:13:12	10.44.1.93	00:21:63:B9:C6:4E	10.44.1.17	Liberty	AnnapolisWireless	disconnect
andrewdjohnson	414.296	11.763	2013-10-20 13:07:14	23 days 02:44:21	10.43.9.169	84:85:06:2b:2f:47	unknown	AWIGateway	AnnapolisWireless	disconnect
andrewdjohnson	148.638	3.355	2013-10-20 13:08:55	23 days 02:42:40	10.43.2.29	b4:f0:ab:d9:a3:b7	unknown	AWIGateway	AnnapolisWireless	disconnect
MikeSievers	4.13	1.712	2013-10-20 21:55:23	22 days 17:56:12	10.44.4.121	c4:43:8f:c3:05:30	10.44.1.17	Liberty	AnnapolisWireless	disconnect
HMWifi1	0.007	0.003	2013-10-21 15:58:24	21 days 23:53:11	10.44.6.53	08:08:C2:72:5F:5B	unknown	Liberty	AnnapolisWireless	disconnect
Kevin1953	99.869	193.715	2013-10-24 19:40:24	18 days 20:11:11	10.42.6.193	58:b0:35:5c:df:13	unknown	BackCreek	AnnapolisWireless	disconnect
justerini	318.243	83.304	2013-10-28 13:24:32	15 days 02:27:03	10.4.4.126	00:26:c7:a1:dd:b6	unknown	Mears Point Marina	MearsPoint	disconnect
danczer	20.072	1.632	2013-10-29 14:00:11	14 days 01:51:24	10.35.4.86	5C:0A:5B:A7:F1:BD	10.35.1.26	Herrington South	AllCity-Wireless	disconnect
danczer	1.396	0.328	2013-10-29 14:10:36	14 days 01:40:59	10.35.2.153	20:68:9D:F8:97:CA	10.35.1.31	Herrington South	AllCity-Wireless	disconnect

Figure 1-1: Active Users Screenshot

1.2.3 Event Viewer

The WiDirect's Event Viewer, which is in the ***System Status*** menu, provides a time line of activity in the network. It shows administrator log-in time, AP status checks, watchdog events, process start/stop actions, client monitoring, and other system activity.

Events are rated on severity, which ranges from ***Info***, ***Alert***, and ***Critical***. If needed, administrators can obtain more detailed event information in the **Reports** section, which allows sorting by severity.

Note: The Event Viewer page also displays the local current system time, which allows administrators to quickly figure out timing of recent events.

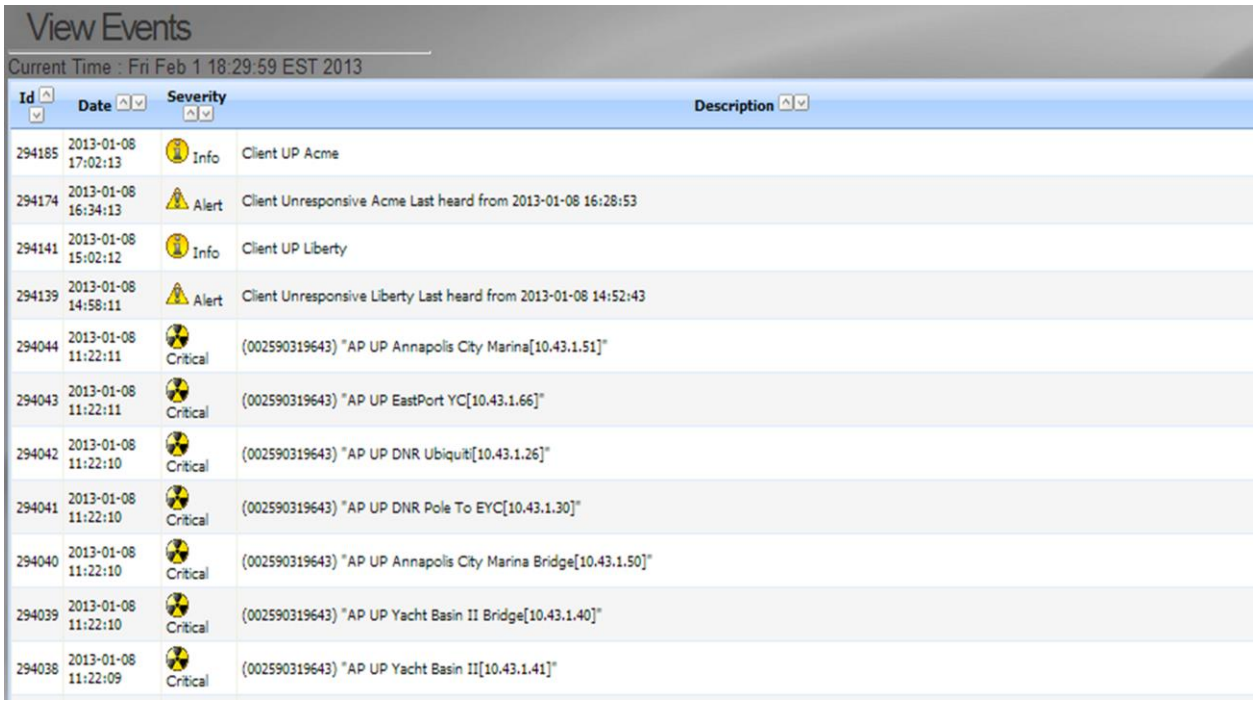


Figure 1-2: Event Viewer Page

1.2.4 AP Status

WiDirect administrators can use the AP Status page, which is under the ***System Status*** menu, to monitor the Access Points on their wireless networks. Access Points are added in the ***System Configuration->Access Points*** menu, which is covered later in this manual. This page only reports the status of configured and enabled access points.

Every Access Point that has been ***enabled*** will automatically be monitored by the WiDirect. This page provides a quick overview of an up/down status of the Access Points, as shown in Figure 1-3. Each AP lists ***Status*** (up/down), ***Name***, ***IP***, and ***Last Ping Time***. If the AP *Name* is clicked, the WiDirect opens the detail page for that AP, which lists all the information that has been gathered via network monitoring. **Last Ping Date** is the last time the WiDirect successfully pinged the AP.

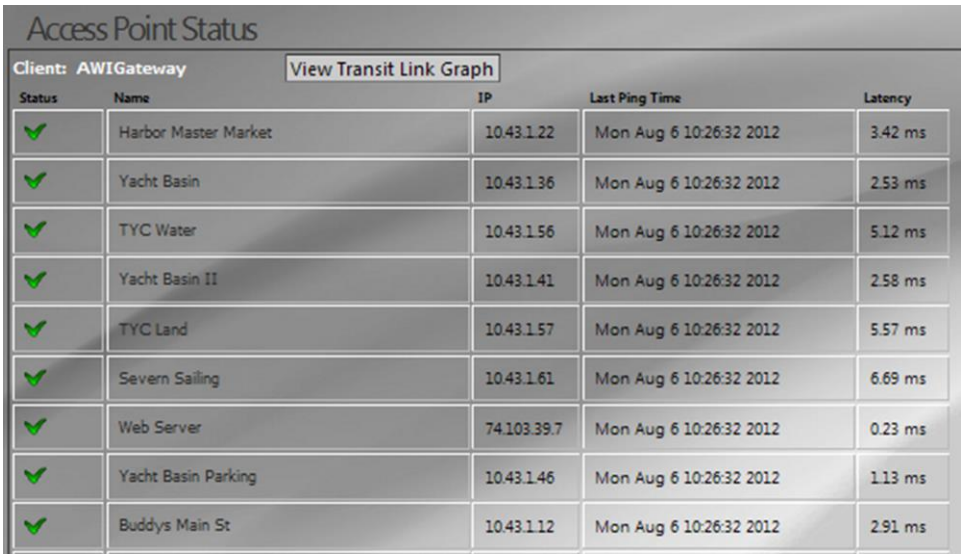


Figure 1-3: AP Status Page

The ***View Transit Link Graph*** button provides a real time view of the wireless mesh TL links. This page not only shows which APs have neighbors, but also provides the TL signal strength and the current number of associated users on the AP. Figure 1-4 shows a sample TL graph link page. Although considered real time, this graph only updates every 5-10 minutes due to the amount of SNMP polling data needed to collect the data.

Note: The TL graph page also displays the serial number of the AP as well as the time the graph was generated.

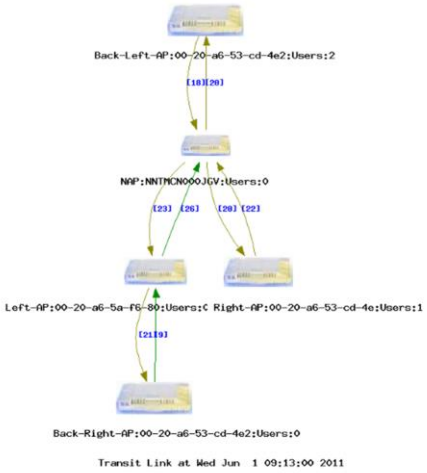


Figure 1-4: TL Graph Sample

1.2.5 Bridge Status

The ***Bridge Status*** page provides a quick overview of the up/down status of the wireless bridges being monitored by the WiDirect. Bridges are added using the same method as adding access points, except their type is set as a bridge. This page only reports the status of access points that are enabled and have their type set as a bridge.

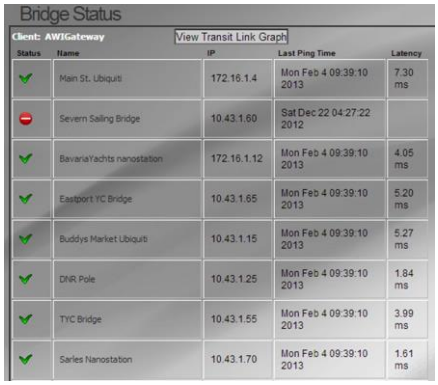


Figure 1-5: Bridge Status Page

1.2.6 Access Point Map Display

Open the View Map link on the AP Status page to view the access points on a map. The map shows all the WiClients and access points. If a location isn't specified for an access point then it will be located near its associated WiClient. When configuring all the access point locations in a large network it is recommended that first the WiClients be moved to their proper location, and then the access points should be moved after the page is reloaded.

Figure 1-6: Access Point Map Display

To move an access point or WiClient simply drag the device to the appropriate location and hit the save button. For the WiDirect to be able to modify the locations of access points on a WiClient a password needs to be set on both the

WiDirect and the WiClient. On the map page on the WiDirect click on ***Main Menu*** and then ***Edit Settings*****.** On a WiClient the ***Map Setup*** link is available under the ***System Config*** **menu.**

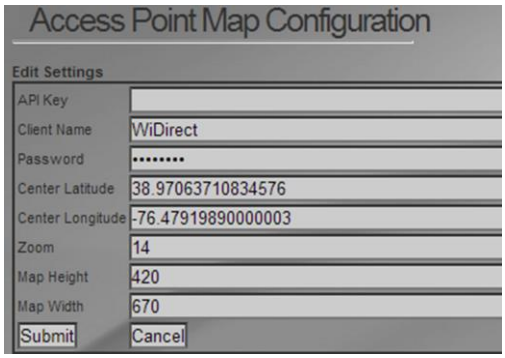


Figure 1-7: Map Configuration

1.2.7 System Check

The ***System Check*** page under the ***System Status*** menu displays a snapshot of the current health of the WiDirect system, as show in Figure 1-6. This page analyzes important system functions, such as **Radius, DNS, DHCP, Firewall, NTPD**, **PreProxy, Squid, and FTP** services by establishing if they are running or not. If for any reason a service has been disabled, click on the **Control** button next to each process in order to re-enable it.

Although the WiDirect has a built in watchdog program that automatically restarts any WiDirect process that has failed, it will not restart any process that the administrator has explicitly stopped. For example, if the administrator stops the **Firewall** via the control window, the watchdog program understands this action and will not attempt to restart the firewall. However, if the Radius process dies, the watchdog will automatically restart the process without Administrator intervention.

Other information that can be found on this page are **Interface Settings, Routing table, NTP status**, and **Network statistics.** Information here can indicate configuration errors if errors or dropped packets are reported. When contacting technical support, the data on this page will be used to troubleshoot the health of the WiDirect.

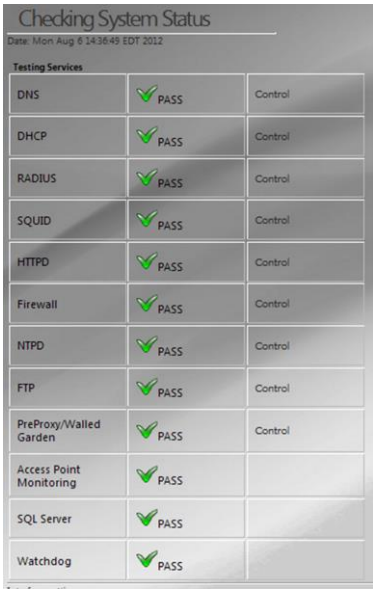
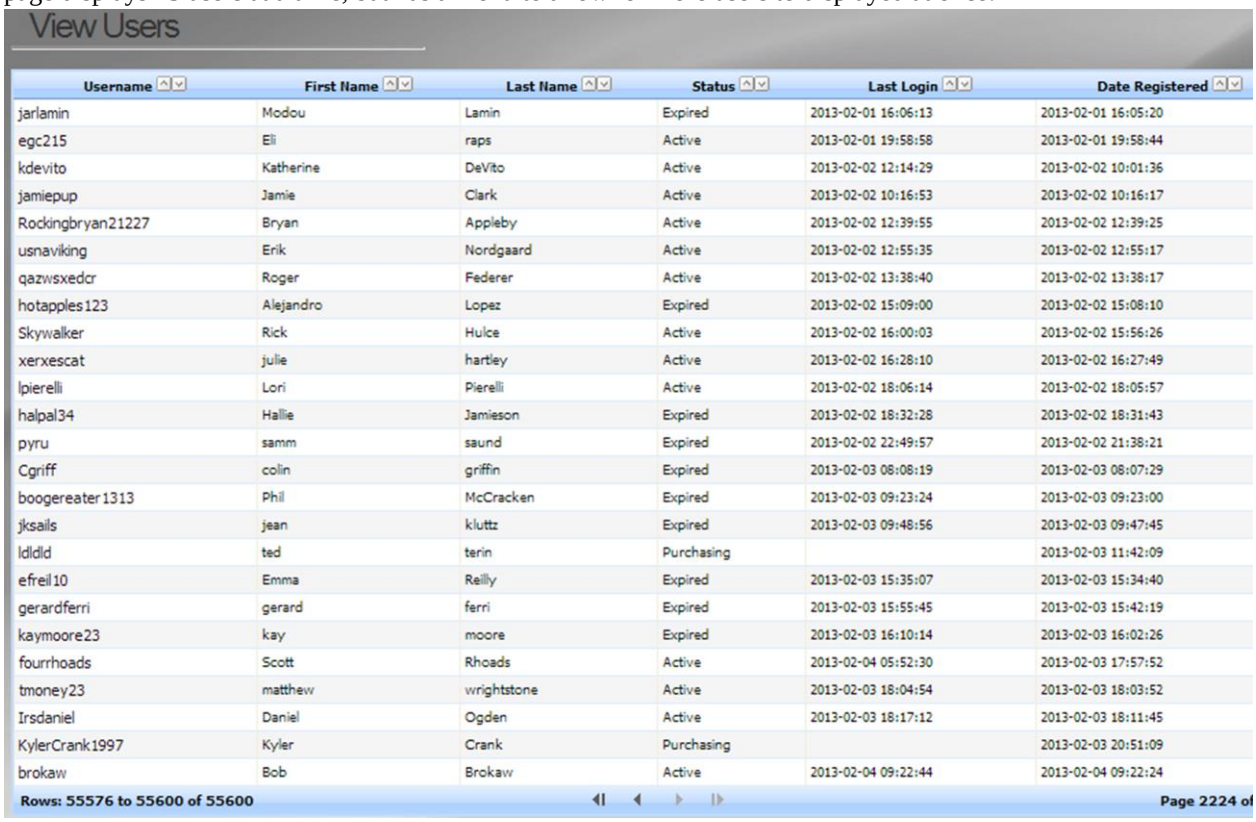


Figure 1-8: System Check

1.3 Users Menu

1.3.1 Viewing All Users (List All**)**

Clicking on the ***Users->List All*** menu provides an extensive list of all users currently in the WiDirect database. This page displays 25 users at a time, but has a menu to allow for more users to displayed at once.



View Users

Username	First Name	Last Name	Status	Last Login	Date Registered
jarlamin	Modou	Lamin	Expired	2013-02-01 16:06:13	2013-02-01 16:05:20
egc215	Eli	raps	Active	2013-02-01 19:58:58	2013-02-01 19:58:44
kdevito	Katherine	DeVito	Active	2013-02-02 12:14:29	2013-02-02 10:01:36
jamiepup	Jamie	Clark	Active	2013-02-02 10:16:53	2013-02-02 10:16:17
Rockingbryan21227	Bryan	Appleby	Active	2013-02-02 12:39:55	2013-02-02 12:39:25
usnaviking	Erik	Nordgaard	Active	2013-02-02 12:55:35	2013-02-02 12:55:17
qazwsxedcr	Roger	Federer	Active	2013-02-02 13:38:40	2013-02-02 13:38:17
hotapples123	Alejandro	Lopez	Expired	2013-02-02 15:09:00	2013-02-02 15:08:10
Skywalker	Rick	Hulce	Active	2013-02-02 16:00:03	2013-02-02 15:56:26
xerxescat	julie	hartley	Active	2013-02-02 16:28:10	2013-02-02 16:27:49
lpierelli	Lori	Pierelli	Active	2013-02-02 18:06:14	2013-02-02 18:05:57
halpal34	Hallie	Jamieson	Expired	2013-02-02 18:32:28	2013-02-02 18:31:43
pyru	samm	saund	Expired	2013-02-02 22:49:57	2013-02-02 21:38:21
Cgriff	colin	griffin	Expired	2013-02-03 08:08:19	2013-02-03 08:07:29
boogereater1313	Phil	McCracken	Expired	2013-02-03 09:23:24	2013-02-03 09:23:00
jksails	jean	kluttz	Expired	2013-02-03 09:48:56	2013-02-03 09:47:45
ldldld	ted	terin	Purchasing		2013-02-03 11:42:09
efreil10	Emma	Reilly	Expired	2013-02-03 15:35:07	2013-02-03 15:34:40
gerardferri	gerard	ferri	Expired	2013-02-03 15:55:45	2013-02-03 15:42:19
kaymoore23	kay	moore	Expired	2013-02-03 16:10:14	2013-02-03 16:02:26
fourrhoads	Scott	Rhoads	Active	2013-02-04 05:52:30	2013-02-03 17:57:52
tmoney23	matthew	wrightstone	Active	2013-02-03 18:04:54	2013-02-03 18:03:52
Irsdaniel	Daniel	Ogden	Active	2013-02-03 18:17:12	2013-02-03 18:11:45
KylerCrank1997	Kyler	Crank	Purchasing		2013-02-03 20:51:09
brokaw	Bob	Brokaw	Active	2013-02-04 09:22:44	2013-02-04 09:22:24

Rows: 55576 to 55600 of 55600 Page 2224 of

Figure 1-9: List All Users

This screen shows a snapshot of all users stored in the database, displaying their username, first and last names, status (active, expired, etc.), the date of their last login, and the date they registered. Clicking on a username brings up the user's edit profile page, which provides all of the user's account information.

1.3.2 Find User

If a customer forgets their login information, or wants to update their profile, this page allows administrators to quickly search for that user's account.

To find a user, enter at least one piece of information about the user, such as username, last name, first name, email address, password, or MAC address and click the *Lookup User* button. The WiDirect will search the database for the information provided and display any matches that it finds.

Figure 1-10: Find User

1.3.2.1 Find User Wildcards

Wildcard searches are supported with the character %. For example:

- Find a username that begins with b and ends with y, use "b%y"
- Find a username that contains the word smith, use "%smith%"
- Find all email address that end with hotmail.com, use "%hotmail.com"

If multiple matches are found on the provided search criteria, the WiDirect provides the administrator with a list of all matches.

1.3.3 Add User

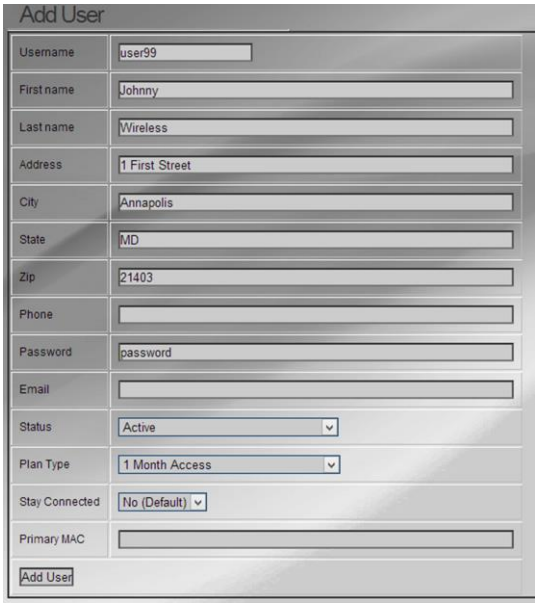


Figure 1-11: Add User

An administrator can use the ***Add User*** page to add a user to the WiDirect's local user database. Most fields are self-explanatory with the exception of **Status**, **Plan Type**, **Stay Connected**, and **Primary MAC**.

Status can be Active, Disabled. Expired, or Purchasing. Table 1-2 describes all the possible user status codes.

Active	The user is fully activated and ready to use the system without further configuration.
Disabled	The user has been effectively banned from the network and can never login without administrator help.
Expired	The user's plan has expired and the user will be asked to select or purchase a new plan upon their next network login.
Purchasing	The user has been registered but has not purchased a plan, which is useful for creating an account and still having the user to be challenged for a plan selection on their next login.

Table 1-2 User Status Types

Plan Type is the plan the user is currently using. If a user is added and set to active, then a valid plan must be selected. The WiDirect shows all active plans in the pull down menu for this item.

Primary MAC is the MAC address of the user. This entry is only important if MAC based authentication has been enabled and can normally be left blank by the Administrator when adding a new user. The WiDirect will automatically populate this field upon the user's next valid login to the network.

Stay Connected determines whether or not the user is disconnected from the system after reaching the maximum connection time. If this option is enabled then the user will remain connected until the account is marked as expired.

1.3.4 **Banning MAC Addresses**

In the event that a computer is found to be engaged in malicious or unfavorable behavior, an administrator can ban the MAC address from the network via the *MAC-Banned* page under the ***Users*** menu. On this page, simply click **Add MAC,** then enter the MAC address to ban.

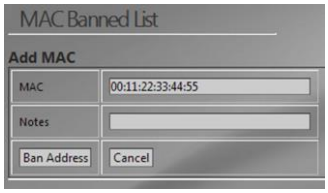


Figure 1-12: Banning a MAC from the network

Administrators can also remove bans from this page by clicking the **delete** button next to the MAC address.

1.3.5 Viewing User Details

When on the *Active Users* page, or the *Find Users* page, click on an individual user to bring up their details. The user details screen, which is shown in Figure 1-13, shows the registration information for the user. From that page the user's information can be updated, or their status can be changed to expired to mark their account as inactive. This page also lists each of the plans the user is active on, and gives the option to expire any of those active plans. If the user is expired then the most recent expired plan will be displayed. Update any of that information and click the **Update User Information** button to update the user's account information.

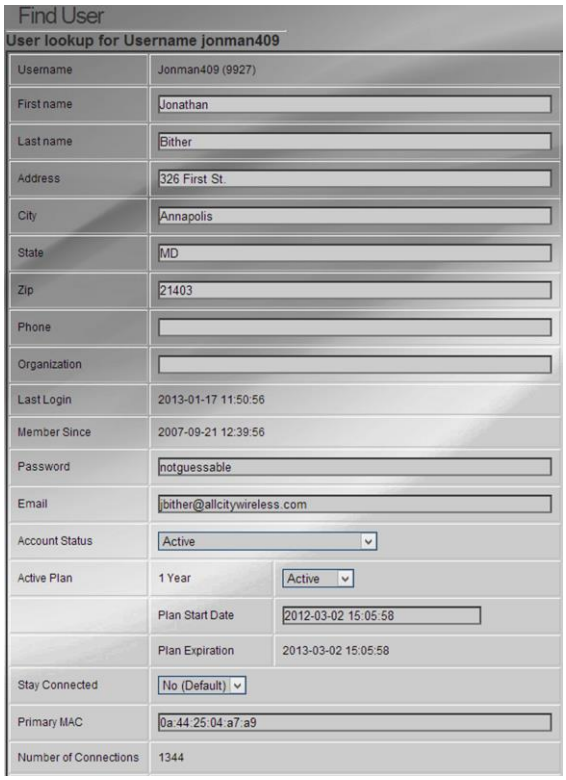


Figure 1-13: View User Details

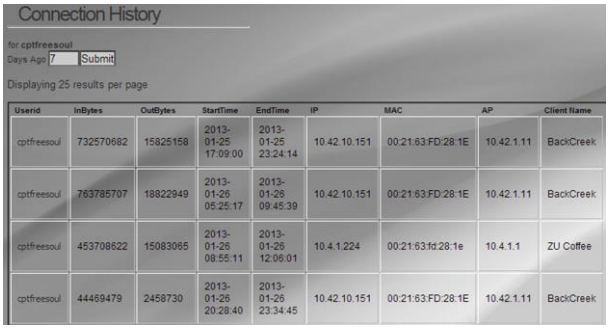
It is important to use the **Change User Plan** option when activating a user's account. Simply changing the user's status to be active on the top part of the form does not update the user's registration date. If an account was previously automatically expired, and the administrator simply changes their status to be active again, then the user's account will be automatically expired again. If the user is on a recurring plan then this action could cause the user's credit card to be charged again. To activate a user you should select the new plan and click the **Update Plan** button. This action will update the user's registration date to be the current time.

The bottom of the page gives additional operations that can be performed on the user. Click the **Delete This User** link to delete the user from the database. That option may not be available if the user has an active recurring subscription. In that case a **Delete Payment Profile** option will also be available to remove that user's payment profile. To view the user's connection history click the **View Connection History** link. The user can be disconnected by pressing the **Disconnect** link.

The user details page also allows the administrator to add additional MAC addresses to associate with the account. These entries may also be populated automatically if the user is on a plan that has a restriction on the number of devices. When adding a MAC address to an account check the "Authenticate Automatically" checkbox for devices that don't have web browsers to have those devices automatically authenticate as soon as they make a DHCP request.

1.3.6 View User's Connection History

From the user details screen you can click the **View Connection History** link to view a user's connection history. By default the page shows the user's connections for the past 7 days. The connection history page shows when the user was connected, how much data they transferred, and which client they were connected on.



Userid	InBytes	OutBytes	StartTime	EndTime	IP	MAC	AP	Client Name
cptfreesoul	732570682	15825158	2013-01-25 17:09:00	2013-01-25 23:24:14	10.42.10.151	00:21:63:FD:28:1E	10.42.1.11	BackCreek
cptfreesoul	763785707	18822949	2013-01-26 05:25:17	2013-01-26 09:45:39	10.42.10.151	00:21:63:FD:28:1E	10.42.1.11	BackCreek
cptfreesoul	453708622	15083065	2013-01-26 08:55:11	2013-01-26 12:06:01	10.4.1.224	00:21:63:fd:28:1e	10.4.1.1	ZU Coffee
cptfreesoul	44469479	2458730	2013-01-26 20:28:40	2013-01-26 23:34:45	10.42.10.151	00:21:63:FD:28:1E	10.42.1.11	BackCreek

Figure 1-14: View User's Connection History

1.4 User Experience Menu

1.4.1 Preferences

The P**references** page, shown in Figure 1-15, allows an Administrator to define the look and feel for users of the network. For example, the redirect page field forces each user to see a specific web page upon logging onto the network. This configuration might work for attendees at a conference to see the day's events, an apartment community to see the rules and regulations, or even to display a splash page of advertisements.

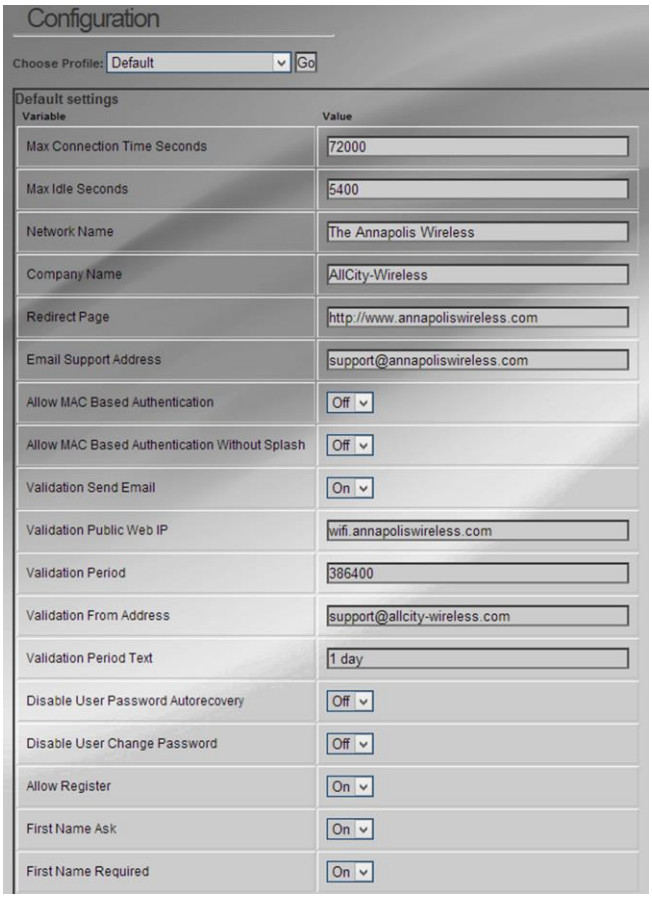


Figure 1-15: Preferences

The default entries for each field, which are described in the table below, provide the default behavior of each setting. Administrators can override each setting at the profile level. If an entry is configured in the profile settings submenu, the profile level setting will be used if the user connects to the profile. To choose a profile to modify select from the list at the top and press the Go button.

If no setting is configured in the Profile settings submenu, the default setting will be used.

Field Dependencies - (Default vs. Per Profile) User experience preferences can be either a global default setting or Profile specific parameters.

Max Connection Time Seconds	The maximum connection time, in seconds, before a user is disconnected and needs to login again. This setting is useful for advertisement based networks, where users should view the login ads at intervals.
Max Idle Seconds	Maximum time in seconds that an idle user is allowed to be connected. If no traffic is passed on their connection, they are considered idle. Once idle for this many seconds, they are disconnected from the WiDirect.
Network Name	Name of the network. It is displayed in the login page, the terms and conditions on the registration page, and where

	ever the %NETWORK_NAME% variable is used on the branding pages.
Company Name	Name of the ISP. It is used in the branding wherever the %COMPANY_NAME% variable is used.
Redirect Page	The page the user is redirected to upon logging into the network. Leave this field blank to redirect user to their originally requested URL.
Email Support Address	Email address displayed to the user in branding.
Allow MAC Based Authentication	This setting allows the user to bypass entering a username and password on the login page. The user must still start their browser to be 'logged' into the system. The firewall must be properly configured in order for a user's MAC address to be determined automatically.
Allow MAC Based Authentication Without Splash	This setting allows users to be authenticated via radius and DHCP messages. As soon as a user is connected to the mesh, they will be authenticated into the system without starting a browser. In order for this setting to work properly, the **Allow MAC Based Authentication** option must also be enabled and the **getapfromradius** must be set in the firewall configuration. See firewall section for more information
MAC Authentication Automatically Create Accounts	This option can be enabled to automatically create accounts for users, which can be used to display a simple splash page or terms and conditions page to the user before accessing the network. To use this option MAC authentication must be enabled and the option to collect usernames and passwords must also be disabled. Additionally, only one access plan should be available for the profile.
MAC Authentication Display Proceed Page	Controls whether or not users who are authenticated by their MAC address see a splash page with a button to click to continue. This page gives a chance to display network information or policies.
Validation Send Email	This setting tells the WiDirect to send a welcome email to the user. In this email the user is asked to verify their email address by clicking on a link.
Validation Public Web IP	The public IP or domain of the web server, which is used in the verification emails sent to newly registered users. In the email the user is asked to click on a URL at this domain to validate their account. This setting must also be properly filled in to accept payment through Authorize.net or PayPal. This field sets the domain of that URL
Validation Period	This setting is currently unused by the system and is for customers who request this feature. If this feature is enabled by AllCity Wireless Support, it will define the number of seconds (usually 1 day or more) that the user has to click on the validation email URL before their account is disabled.

	In other words, if they do not validate their email address by clicking on the URL in the validation email, their account will be suspended until they do.
Validation From Address	The email address from which the user sees verification emails originate.
Validation Period Text	The amount of time in text format that is displayed to the user in the validation email. Instead of displaying the number of seconds that are defined in the **Validation Period** setting, this option allows the administrator to define a more human readable form of the amount to time. For example, '1 day' might be a more desirable value than 38640 seconds.
Disable User Password Autorecovery	If set to yes, the "Forgot Password?" link will be removed from the login page. This setting is a security parameter that can be used at the administrator's discretion.
Disable User Change Password	If set to yes, the "Change Password" link will be removed from the login page.
Allow Register	Set this value to no to hide the link on the login page for users to create an account.
First Name Ask **First Name Required** **First Name Text** **Last Name Ask** **Last Name Required** **Last Name Text** **Org Ask** **Org Text** **Org Required** **City Ask** **City Text** **City Required** **State Ask** **State Text** **State Required** **Zip Ask** **Zip Text** **Zip Required** **Phone Ask** **Phone Text** **Phone Required** **Extra Ask** **Extra Text** **Extra Required** **Terms and Conditions Ask** **CAPTCHA Ask**	These options allow for customization of the registration process for new users of the network. Each of the standard fields can be changed to ask for something different, or disabled completely. There are also three extra fields, which can be customized for any additional information that is to be collected. The CAPTCHA, a security code used to prevent automated registrations, can also be enabled to prevent automated account registrations. If the CAPTCHA is enabled the user will be asked to enter the text from an image on the registration page. The text of the terms and conditions can be edited in the profile branding section.
Show Login Text	If turned off then there is more control over the look of the initial login page as much of the extra text will no longer be included. If turned off the login form will contain the minimum amount of required text to login, such as social media options or the username and password fields.
Show Login Page	Turning this option off will simply redirect the user straight to the registration page if they don't already have an

	account. MAC authentication must be enabled to allow users to authenticate automatically after an account is created.
Collect Username and Password	The collection of usernames and passwords can be disabled if authenticating users based on their MAC address.

Table 1-3: Preferences Options

1.4.2 Walled Garden

The WiDirect's ***Walled Garden*** allows administrators to host content (e.g., community website) that can be integrated into the captive portal-landing page. For example, administrators might want their users to be able to go to google.com without network authentication. In order to allow this, only ".google.com" needs to be added to the Walled Garden list. The WiDirect can also be configured to automatically search for web pages to add to the walled garden. This feature allows for the user to browse not only that web site, but also all the sites linked from that web site. If some sites do not need to be crawled as deeply as others, the depth to be crawled of each site can be specified on the same line as the site. As the Walled Garden Crawler may not be able find all sites that are needed to display a web page properly, it is a good idea to test that the pages are displaying correctly and add additional sites as needed.

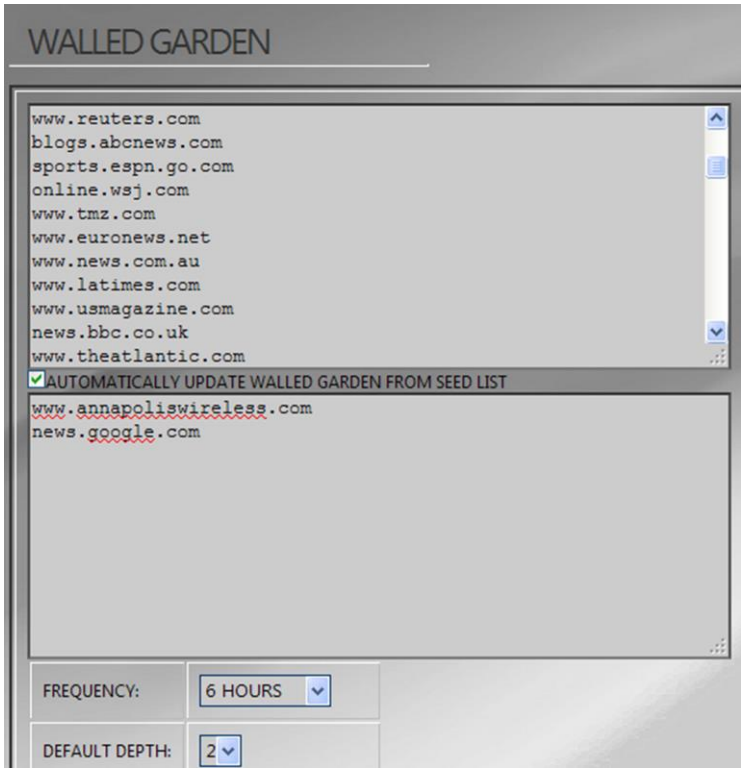


Figure 1-16: Walled Garden

1.4.3 Blocked Sites

The WiDirect has a ***Blocked Sites*** page for the administrator to specify a list of sites that users should be restricted from accessing. Simply add the list of blocked domains, one per line, to the list and click the **Update** button when done. Updating the list of blocked sites will cause a service outage of about 30 seconds.
You can also use that form to upload a list of sites to be blocked from a text file. The text file should be a plain text file, with one domain per line.
Note: Content filtering is not available by default on the Micro WiDirect or Micro WiClient. Use of firewall rules or a DNS filtering service is encouraged for content filtering on these devices.

1.4.4 Message of the Day

The ***Message of the Day*** *(MOTD)* feature allows administrators to create a message that appears on the login screen. When the user is prompted for the username and password, the message of the day will also be displayed depending on how the branding is configured. See the branding section for more information on how the MOTD is displayed on the login screen.

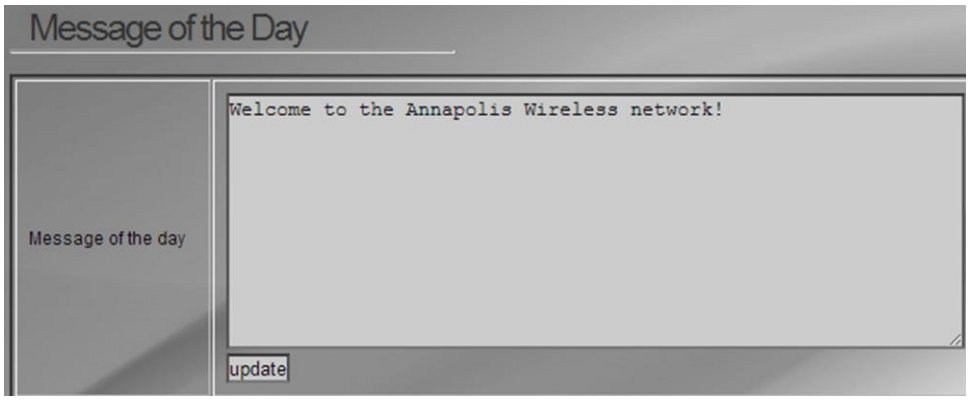


Figure 1-17: Message of the Day

The entire MOTD field can accept HTML code. However, only hyperlinks, <font>, <p>, and <br> tags should be used to keep any distortion to a minimum. Any external links added to the MOTD need to be in the walled garden or in the firewall configuration.

1.4.5 Profile Branding

All WiDirect units come with a default set of fully implemented authentication portal pages. This is a completely functional Captive Portal and can be used to perform all needed authentication related functions. New users may sign up through this portal by entering their desired login/password, name, contact information, and billing information. The default portal may be modified to include customized graphics and textual information such as usage agreements and contact information.

Figure 1-18: Sample Login Page

To customize these Authentication pages, click on *Profile Branding* link under the *User Experience* menu. From here, select which Profile to change the branding on the branding edit page.

Select the **Preview** button to view what the login, Forgot Password, Change Password, and Register pages will look like to users with this branding.

Figure 1-19: Profile Branding Selection

When a profile is selected from the Branding Selection page, a new page is shown that lists each possible brandable page, as shown in Figure 1-20.

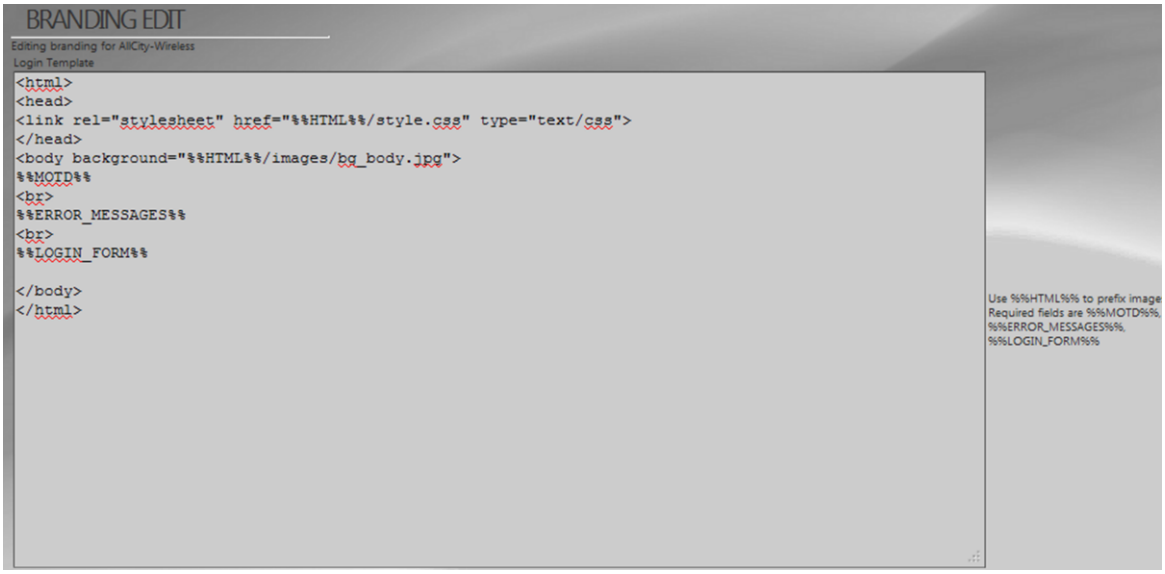


Figure 1-20: Profile Branding

On this page, there are Login, Register, Purchase, Terms & Conditions, Forgot Password, Change Password, Expired Page, Stylesheet, and Verification email templates. Each page supports certain keywords, and has a list to the right that describes which variables are valid for that page. Additional custom variables are available as well. On the Profile Branding page custom variables are listed under the advertisements heading. Advertisements allow you to make the change in one place and have the text on multiple pages changed at one time.

For example, the Login page allows the following variables:

%%HTML%%	Available on all branding pages. Used when referencing images and other files existing on the WiDirect. See the Using Images in Branding section below for more information. NOTE: This must also be used when referencing the CSS stylesheet. See the example branding file below as an example.
%%MOTD%%	The WiDirect replaces this with the text from the MOTD.
%%ERROR_MESSAGES%%	If there was an error message, such as "Incorrect Password", this variable tells the WiDirect where to place that information.
%%LOGIN_FORM%%	Where the login form will be displayed. This variable IS REQUIRED for the login branding page.

Table 1-4: Login Form Branding variables

There are a number of different pages that can be modified from the profile branding page. Not all of these are used in every deployment. Table 1-5 describes each of the templates that can be modified.

Login Template	The initial splash page the user is brought to.
Register Template	The registration page where all the information is entered.
Register Welcome Template	The successful registration page.
Purchase Template	The template for the various purchase pages. Includes the plan listing page, as well as the credit card entry pages.
Terms and Conditions	The terms and conditions that is displayed on the registration page.
Forgot Password	The page for the user to lookup a forgotten password.
Change Password	The page for a user to change their existing password.
Expired Page	The expired page is where the user is asked to verify their email address when reactivating an account.
Blocked Page	If the user tries to access a blocked site then they will be brought to the blocked page.
Advertisement Page	If an advertisement interval is set for the plan then the users will see the advertisement page regularly.
Facebook Template **Google Template** **LinkedIn Template**	These pages are used for users of iOS devices to make the end user experience more fluid for the end user. When the user clicks the button to login with a social media provider they are first brought to this intermediate page before clicking through one more time to authenticate with their provider.
Update Credit Card	This page is used for updating a previously saved credit card when using Authorize.net CIM for automatic payments.
Style Sheet	The style sheet that can be included by the other pages.
Verification Email	This email is sent to a new user to welcome them to the network.
Successful Payment Email	This email is sent to a user after a successful recurring payment. It is not sent for one time payments, or for the initial payment on a recurring plan.
Failed Payment Email	This email is sent to a user after a failed recurring payment. This email should include a link to the update credit card page for the user to update their payment details.

Table 1-5: Available Branding Templates

The following is a sample login branding page. All the variables have been bolded to make it easier to read.

```
<html>
<head>
<link rel="stylesheet" href="%%HTML%%/style.css" type="text/css">
</head>
<body background="%%HTML%%/images/bg_body.jpg">
<table width="500" border="0" align="center" cellpadding="0" cellspacing="0">
 <tr>
  <td><table width=500 cellspacing="0" cellpadding="0" border="0">
   <tr>
    <td width="32"><img src="%%HTML%%/images/logo.jpg"></td>
    <td  width="468"><a  href="http://www.annapolis-wireless.com/contact.html"  target=_blank><img
src="%%HTML%%/images/banner.jpg"  border=0></a></td>
   </tr>
   <tr>
    <td bgcolor="#ad0006"></td>
    <td bgcolor="#ad0006"></td>
   </tr>
   <tr>
    <td><img src="%%HTML%%/images/photo1.jpg"></td>
    <td><img src="%%HTML%%/images/photo2.jpg"></td>
   </tr>
   <tr>
    <td colspan=2><h3>%%MOTD%%</h3></td>
   </tr>
  </table>
   <table width="500" border="0" cellspacing="0" cellpadding="0">
    <tr>
     <td width="200"><br>
      %%ERROR_MESSAGES%% <br>
      <br>
      %%LOGIN_FORM%%</td>
     <td  width="300"><iframe  scrolling="no"  frameborder="0"  width="300"  height="250"
src="http://adserver.allcitywireless.com"></iframe></td>
    </tr>
   </table>
  <p> </p></td>
 </tr>
</table>
</body>
</html>
```

1.4.5.1 Using Images in Branding

On the **Branding Edit** page, there is also an area at the bottom of the screen that allows images to be uploaded. After uploading, the images can be referenced in any of the branding pages (except stylesheet) by using the following convention:

```
<img src="%%HTML%%/images/imagename.gif">
```

The i*magename.gif* is the name of the image to be displayed. The WiDirect will automatically replace %%HTML%% with the correct URL information. If the %%HTML%% keyword is not listed, the image will not be displayed correctly.

WARNING: Be careful about HTML construction. If unsure, administrators can use the preview button to view what the branded pages look like.

Just about anything can be changed, including the login form, by editing the Stylesheet portion of the branding. With the exception of the variables described in the previous section, any HTML code is valid in the branding pages. Unfortunately, listing all the possible HTML tags is outside the scope of this document. To learn more about HTML tags and page construction, see the guide at http://www.w3schools.com/html/

1.4.6 Radius

The Radius page is used to control the Radius server queried by each profile. Typical WiDirect installations will not need this function, and the settings can be left as their default. Radius servers can be set for specific profiles, or can be global settings for all users. See the chart below for a description of each of the fields. Typically all the options should be set to "On" when using Radius authentication.

Radius attempt authentication	Controls whether or not Radius authentication is enabled for this profile.
Radius add users not in DB	Set to yes when using Radius authentication for users to be added to the database properly. Setting this option to no will only allow users who already have accounts on the system to authenticate against the Radius server.
Radius replace users in DB	Set this option to yes to allow the user override any local user accounts.
Radius authentication primary	This option controls whether the Radius authentication will take priority of local user accounts. Set to yes to disable authentications against the local database.
Radius save password	This option can be set to no to prevent the WiDirect from saving the password for authenticated users. Should only be used when local database authentication is disabled.
Radius default user plan	The plan that users will be assigned to when authenticating.
Radius secret	Shared secret for the Radius server.
Radius server	IP or hostname of the Radius server.
Radius authentication port	Port for radius authentication (1812)
Radius accounting port	Port for radius accounting (1813)
Radius account prefix	Prefix added to account names in WiDirect database for Radius accounts. This prefix can be used to allow local users to be created with the same names as the Radius database. It is recommended to use character that cannot typically be used in an account, such as a hyphen. Example prefix: radius-
Radius authentication method	Various Radius authentication methods.
Radius secondary server enabled	Turn this option on to use the secondary server. The primary server must be enabled to use a secondary server. The same options described above are available for the secondary server

Table 1-6: Radius configuration

1.5 Social Networking

1.5.1 Overview

The WiDirect allows for integration with various social media providers. If a user is already logged in to Facebook or Google+ they can register an account on the WiDirect in seconds. Some basic information is obtained from them based on what their permissions allow. Configuring this type of authentication requires following the steps to create an application on the desired social media provider and then entering the details on the WiDirect. It is also important that the firewall be properly configured to allow for social media access as by default access to all sites except for the WiDirect is restricted. See section 1.8.4 for details on configuring the firewall.
These steps require an actual domain be used on the WiDirect, which will also be configured on the firewall page. For information on using a locally created domain name consult the WiDirect support web site. The examples that follow will use widirect.example.com for the domain, so the valid domain should be substituted in for widirect.example.com.
These steps will typically refer to the default WiClient and WiDirect installation where all path names use /portal/. In a Cloud WiDirect environment a different path name will be used instead of /portal/. When deploying in a cloud environment please use your actual path name instead of /portal/.

1.5.2 Facebook

1.5.2.1 Create Facebook Application

The Facebook application can be created at https://developers.facebook.com. The options to create an application are under the Apps menu. Facebook will first ask you to register as a developer before allowing you to create apps. It is important to understand their privacy policy and what you can do with the data collected. Remember to use a Facebook account that you will have access to later in case you want to change settings or view the reports.

After registered as a developer you can select the option to "Create a New App." For the Display Name select a name you would like displayed to users. Choose any category and click the "Create App" button. You will then be prompted to enter a security code before proceeding.

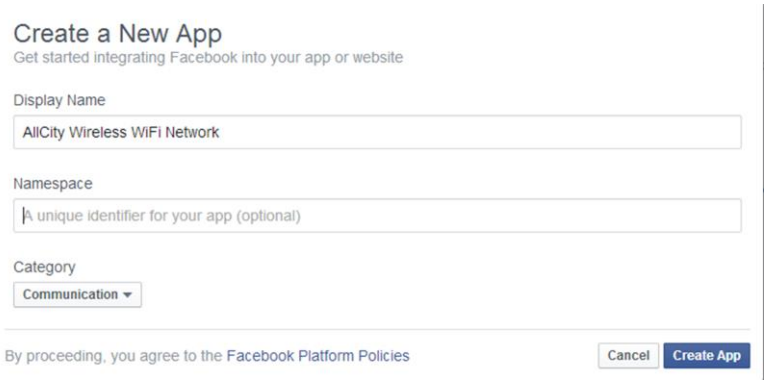


Figure 1-21: Facebook App Creation Screen

After creating the application open the Settings page. Choose the option to “Add Platform” and then choose “Website.” After adding the platform the next step will be to fill in the values on the Settings page. The table below describes what needs to be entered.

App Domains	Enter the domain for the WiDirect.
Site URL	Enter the domain for the WiDirect.
Contact Email	Email a contact Email address for updates about this app.

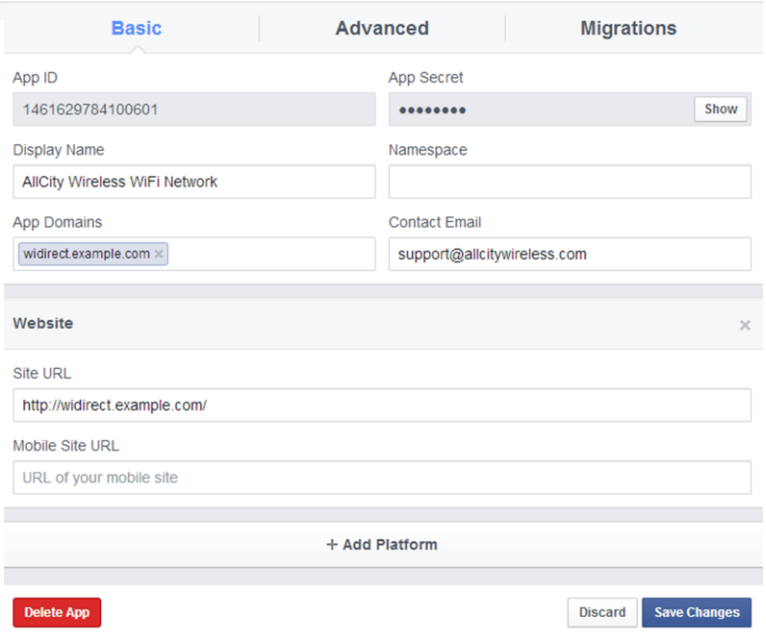


Figure 1-22: Facebook App Settings Screen

Once finished entering the proper options on the Settings page it may be a good idea to record the App ID and App Secret for use later. Hit the “Show” button to view the secret. These values will be used later on when configuring the app on the WiDirect. Be sure to hit the “Save Changes” before moving on to the next step. Open the Status & Review page and update the option at the top to make the app available to the general public.

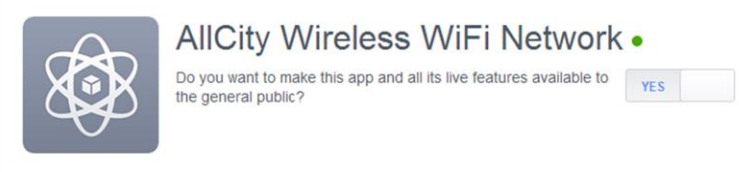


Figure 1-23: Facebook Status & Review Page

1.5.2.2 Configure WiDirect Settings

After the Facebook app is created the necessary settings can be entered in the WiDirect. On the Facebook Settings page choose a profile and hit the "Go" button to modify the settings for a specific profile, or leave the profile as the default option to modify the Facebook settings for all profiles. The App ID and secret are the values from the Facebook App Settings screen shown on the previous page. The Facebook Site URL should simply be "http://" followed by the domain being used, such as "http://widirect.example.com".

1.5.3 Google+

1.5.3.1 Configure Google+ Settings

Visit Google Developers Console, https://console.developers.google.com/project and create a new project.

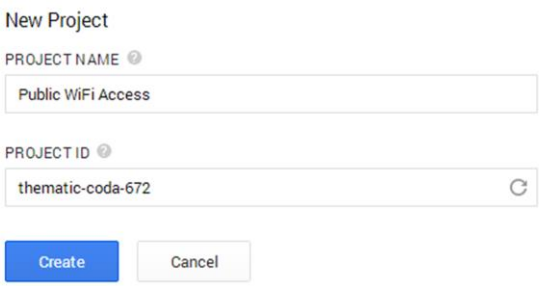


Figure 1-24: Google App Creation Screen

Choose a name for the project ("Public WiFi Login"). Then click on Consent screen under "APIs & auth." On the consent screen choose an email address and enter a name for the product. The users will see the name entered here when they first connect to the network.

Next click on Credentials under "APIs & auth" to open the page for getting the necessary values for entering in to the WiDirect. Then click "Create a new Client ID" and the table below will describe the values that need to be entered. After hitting the "Create Client ID" be sure to record the Client ID and Client Secret values for entry in the WiDirect.

Application type	Web application
Authorized Javascript origins	Enter the domain of the WiDirect. If not using an SSL certificate then be sure to update the protocol to be http instead of https.
Authorized Redirect URL	Enter the domain of the WiDirect followed by "/portal/login/googlecallback.php". If not using an SSL certificate be sure http is specified at the beginning of the URL. In a Hosted WiDirect environment the /portal/ may also need to be change to the path name being used.

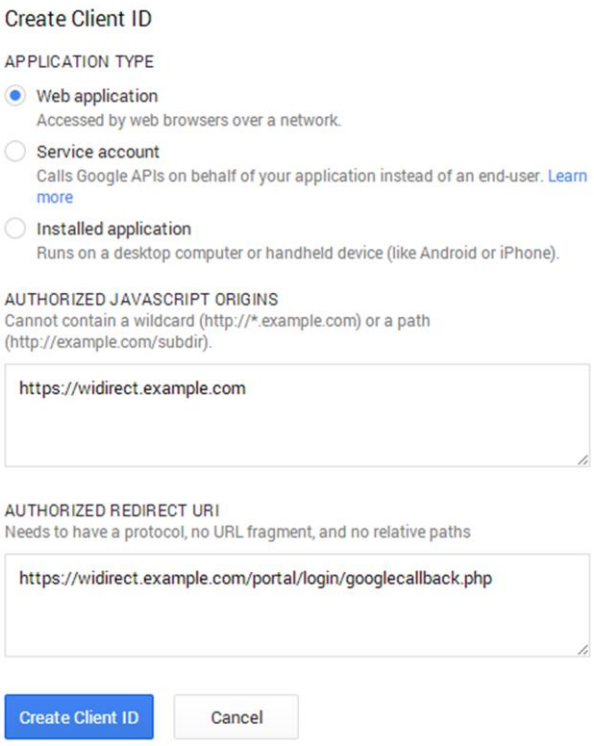

Create Client ID
APPLICATION TYPE
Web application
Accessed by web browsers over a network.
Service account
Calls Google APIs on behalf of your application instead of an end-user. Learn more
Installed application
Runs on a desktop computer or handheld device (like Android or iPhone).
AUTHORIZED JAVASCRIPT ORIGINS
Cannot contain a wildcard (http://*.example.com) or a path (http://example.com/subdir).
https://widirect.example.com
AUTHORIZED REDIRECT URI
Needs to have a protocol, no URL fragment, and no relative paths
https://widirect.example.com/portal/login/googlecallback.php
Create Client ID
Cancel

Figure 1-25: Google App Creation Screen

1.5.3.2 Configure WiDirect Settings

On the Google+ settings page choose the desired profile and enter the Client ID and Client Secret generated previously. The Google Redirect URL should be /portal/login/googlecallback.php at the desired domain, such as "http://widirect.example.com/portal/login/googlecallback.php". In a Hosted WiDirect environment be sure to update the path from /portal/ to be the actual path name.

1.5.4 LinkedIn

1.5.4.1 Configure LinkedIn Application

To create a LinkedIn application, first go to http://developer.linkedin.com. You may be asked to register as a developer if you have never gone through this process before. Next click on Support and API Keys. Then click "Add New Application."

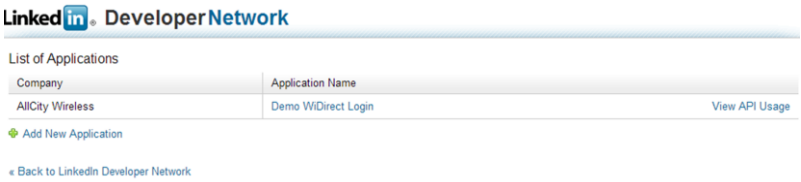


Figure 1-26: LinkedIn App Creation Screen

Company	Choose a company name.
Application Name	Choose a name for the application that the users will see.
Description	Enter any description for the application, such as "Public WiFi Access."
Website URL	Enter a URL for users to find more information about the network. This URL can point to the WiDirect or to any other server.
Application Use	Choose an appropriate option, such as Networking.
Live Status	Set to be Live.
Developer Contact Email Phone	Enter contact Email and phone number for developer related questions.
Default Scope	Be sure these are selected: r_emailaddress, rw_company_admin, rw_groups, r_contactinfo, rw_nus, r_fullprofile
OAuth 2.0 Redirect URLs	Enter the URL like the one below. Substitute in your actual domain name, and if using the Hosted WiDirect service be sure to substitute in the correct path name as well. http://widirect.example.com/portal/login/linkedincallback.php
Agreement Language	Can be left as default to be based on the browser the user is using.
Application type	Web application
Authorized API Domains	Enter the domain of the WiDirect.

After clicking the “Add Application” button the screen will display the details about the configuration of the application. Be sure to record the API Key and Secret Key as they will need to be entered in to the WiDirect.

1.5.4.2 Configure WiDirect Settings

On the LinkedInsettings page choose the desired profile and enter the API Key and Secret Key generated previously. The LinkedIn Redirect URL should include the protocol and domain, such as “http://widirect.example.com/”.

1.6 Reports

1.6.1 Functionality Overview

The WiDirect is able provide many reports that are useful in both budgeting and planning for future growth. They are also helpful for understanding usage trends, and for reaching out to users for marketing purposes. Reports can help administrators see how much the network is used and where it is used the most. They can also help find potential problems as well as monitor anomalous behavior of equipment or end users.

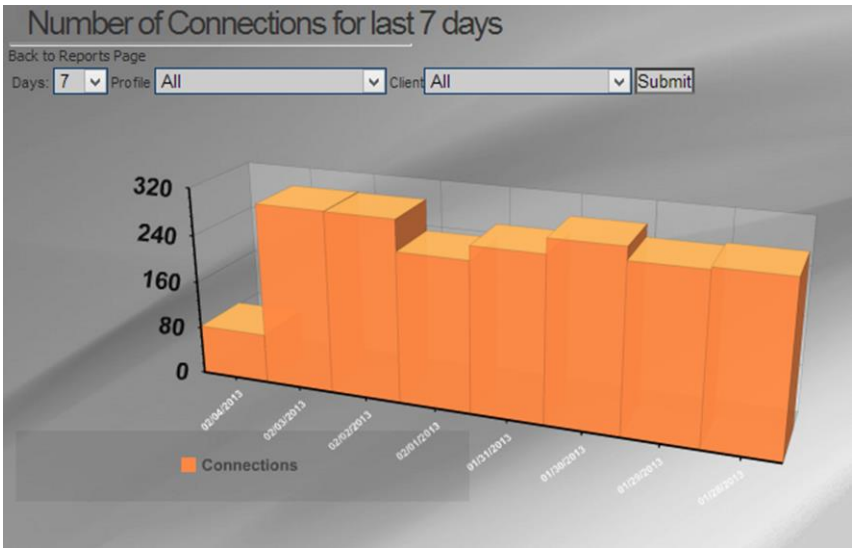


Figure 1-27: Sample Report Output

1.6.2 Connections

The connections report shows connections to a particular profile in increments of 1 to 30 days, monthly, or annually. This report is a representation of how many individuals presented user credentials and were permitted out onto the internet. Another user will show the number of unique users per month. A report is also available to show the manufacturer of the network cards used by the users.

1.6.3 Registrations

The registration report is available in increments of 5 to 30 days, monthly, or annually. This report shows how many people signed up for an access plan in the given period.

1.6.4 Purchases

The purchase reports are available to show daily and monthly totals for the amount of revenue per profile. For more detailed purchase reports click on the link for text based reports.

1.6.5 Overall Usage

The **Overall Usage** tab indicates how much the network has been utilized by each user, sorted in descending order. It will give outputs based on both amount of bandwidth used and time spent on the system for any given date range.

1.6.6 Billing (Purchases)

The end user report that details which user signed up for service by username, the date and time they signed up, and the amount of money associated with the transaction. There is also a confirmation string given that is a unique identifier of the event. For payment gateways such as Authorize.Net, this string is the result code from the actual payment transaction. Otherwise, this string is a unique identifier for each purchase, including free plan purchases.

1.6.7 Access Point Usage

The **Access Point Usage Report** details the amount of usage an Access Point received over a time period. It reports both bandwidth and the number of unique end users. This data is useful in determining whether an AP is in a good location or perhaps might be better deployed elsewhere.

1.6.8 Downloads

Some reports are downloadable as CSV files. These reports include user account information, user e-mail accounts, and event reporting on several severity levels.

1.7 System Configuration

1.7.1 Profiles

To control multiple profiles, they must be defined in the **System Configuration** area of the WiDirect user management console. Once the profile is defined it can use the standard preconfigured look and feel which it receives from the default settings, or it can be customized for different networks or events.

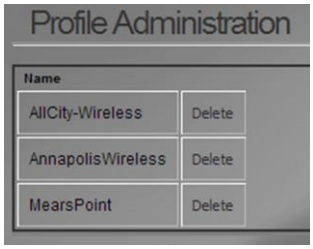


Figure 1-28: Adding Profile

To edit the look and feel of a profile, see the **Branding** discussion earlier in this document.

1.7.2 Access Plans

This page works in conjunction with the local user database and the **Captive Portal.** It allows end users to pick a plan for which they will be billed when they sign up and when they need to recharge their account. A plan is defined by the Administrator and restricts the amount of usage time a user can have.

1.7.2.1 Access Plans Page

The ***Access Plans*** page under the **System Configuration** menu lists the access plans available to end users. Figure 1-21 shows this page, which lists all the currently available plans. To create a new plan, click on the **Add Plan** link.

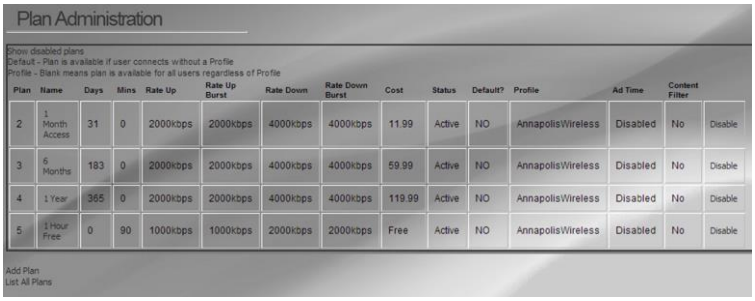

Plan Administration
Show disabled plans
Default - Plan is available if user connects without a Profile
Profile - Blank means plan is available for all users regardless of Profile
Plan Name Days Mins Rate Up Rate Up Burst Rate Down Rate Down Burst Cost Status Default? Profile Ad Time Content Filter
2 1 Month Access 31 0 2000kbps 2000kbps 4000kbps 4000kbps 11.99 Active NO AnnapolisWireless Disabled No Disable
3 6 Months 183 0 2000kbps 2000kbps 4000kbps 4000kbps 59.99 Active NO AnnapolisWireless Disabled No Disable
4 1 Year 365 0 2000kbps 2000kbps 4000kbps 4000kbps 119.99 Active NO AnnapolisWireless Disabled No Disable
5 1 Hour Free 0 90 1000kbps 1000kbps 2000kbps 2000kbps Free Active NO AnnapolisWireless Disabled No Disable
Add Plan
List All Plans

Figure 1-29: Access Plans

1.7.2.2 Adding a Plan

From the ***Access Plans*** page under the *System Configuration* menu, just click on the **Add Plan** link which is located under the list of current Access Plans. This brings up the ***Adding Access Plans*** page, which allows for detailed configuration of a plan. This page is shown in Figure 1-24.

Figure 1-30: Plan Creation

If there is only one free plan defined in the system for a given profile, users will not be given a choice of plan selection. They will be automatically assigned to the single plan.

Table 1-7 describes all the fields for plan creation.

Keyword	**Description**
Name	A descriptive name for the plan. This name is displayed to users on the plan selection page. (alphanumeric field, 1 – 100 characters)
Firewall ID	A unique ID for each plan from 101 to 200. If unsure, use the default number given.
Rank	The rank setting controls the order that the plan is displayed in on the access plan page for the user. It is a dropdown menu containing a hidden option and the values 1-20. Plans with a lower rank will be shown before plans with a higher rank. The hidden option will hide the plan from the users.
Days	Number of days duration a plan is valid for (numeric field, possible values 0 – 999, 0= unlimited)
Minutes	Number of minutes a plan is valid for. This field may be used in addition to the days field. An access plan will only be unlimited if both the days and minutes field are blank (numeric field, possible values 0 – 999, 0= unlimited)
Bandwidth Up	Bandwidth limitation in kbps a user is allowed to upload from their machine. (numeric field, unit of measure: kbps, 0= unlimited)
Bandwidth Up Burst	Bandwidth in kbps a user is allowed to use if extra bandwidth is available, such as when no one else is using the system. For example, you might have a 200 kbps upload limit but a 400 kbps burst limit, which gives users extra bandwidth if available. In most cases this value can be set the same as the bandwidth up setting. **WARNING**: Do not set Bandwidth Up Burst to a value lower than Bandwidth Up setting. (numeric field, unit of measure: kbps, 0= unlimited)
Bandwidth Down	Same as bandwidth limitation in Bandwidth Up, but for defining download speeds. Measured in kbps 1024 would equal 1 megabits (numeric field, unit of measure: kbps,

	0= unlimited)
Bandwidth Down Burst	Same as bandwidth limitation in Bandwidth Up Burst, but for defining the user's download speeds. Measured in kbps. 1024 would equal 1 megabit (numeric field, unit of measure: kbps, 0= unlimited)
Data Limit	The total amount of bandwidth the user is allowed in bytes. After the user exceeds this amount of data their account will be marked as expired. Optionally a throttled bandwidth speed can be applied for the remainder of their plan period. Please consult the WiDirect support site for more information.
Cost	The amount the user must pay in order to receive the plan. If set to zero, the plan will be "Free". (currency field, unit of measure: USD, 0= free) **Note**: To collect payment via the WiDirect, the payment gateways must also be configured.
Recurring	This setting determines whether or not the plan should be automatically billed again after the time expires. In WiDirect Version 2.1 recurring transactions only use the Authorize.net CIM payment gateway.
Occurrences	If the access plan is set to be recurring, then this setting determines how many times the user will be billed.
Default	If the plan is set to default and if no user profile is available or the user's profile doesn't match any plans that are configured specifically for a profile, this plan will be available to the user.
Profile	Applies this plan to a specific profile. Leave blank if the plan applies to all profiles. Enter multiple profiles by separating each with a comma. No extra spaces are allowed.
Ad Interval	The number of seconds in between the display of the advertisement page. Postproxy must be enabled in the firewall configuration file for this feature to work. See section 1.7.4.1 for more details. Interstitial advertisements are not supported on the Micro WiDirect and the Micro WiClient.
Content Filter	Whether or not content filtering is disabled. Postproxy must be enabled in the firewall configuration file for this feature to work. See section 1.7.4.1 for more details. Content filter is not supported on the Micro WiDirect and the Micro WiClient.
Login Allowed on any Profile	If this option is set to Yes, then an account created with this access plan can be used on any profile in the network. If both this option and the Default option are set to No, then accounts created on this access plan will only be able to login on the profile specified in the profile field. This option can be used if one portion of the network allows free access, and the network administrators do not want those users to be able to login on other portions of the network.
Delay Before Repurchase	This option is to limit the frequency that a user may reselect an access plan. Setting this value to 30 would only allow the access plan to be selected once per month. By default this setting will restrict the plan by the MAC address of the user, even if they create another account.
Number of Concurrent Logins	The number of times a user on this access plan is able to login at the same time. If the user signs in on more than this number of computers then all the previous sessions will be disconnected.
Number of Devices	The maximum number of unique devices that a user on this access plan is allowed to use. If they attempt to use more than this many devices their login will be refused. Leave as 0 for no restriction on the number of unique devices an account may have.
Maximum Connection Time	The maximum number of seconds that a user on this access plan is allowed to stay connected. If set higher than 0 this option overrides the maximum connection time for the user's profile.

Maximum Idle Time	The maximum number of seconds that a user on this access plan is allowed to be idle before being disconnected. If set higher than 0 this option overrides the maximum idle time for the user's profile.
Permitted Times	These settings control the times during which a user on an access plan are able to be connected. These fields can be left blank to allow the user to connect with no time restrictions.

Table 1-7: Plan creation fields

1.7.3 Coupons

Coupons can be used as a method to give users access to the network. Each coupon has a description, code, and plan associated with it. The plan associated with the coupon is the access plan the user will be placed on after he or she uses the coupon. The code is what the user enters to activate their account. The description is just used to help categorize the coupons. Multiple coupons with the same coupon code can be added, but the description and access plans also have to be identical. If a coupon is added once then it can be used once. If it is added multiple times then it can be used however many times it was added. Before coupons can be used the coupon payment gateway must be added on the payment gateways screen.

1.7.4 Voucher Admin

This page can be used for adding new administrators for creating vouchers. These administrators do not have access to any of the standard WiDirect administrative functions, and can only create vouchers. These administrators can be limited to creating vouchers only for a specific access plan, and a limit on the number of vouchers created can also be configured. Voucher administrators use a separate URL to access the voucher creation pages:

http://10.4.1.1/portal/voucher/

See section 1.11 for a full description of the Voucher Management System.

1.7.5 Access Points

On the ***System Configuration->Access Points*** menu, this page allows administrators to list all the access points and bridges configured on their network. By entering an access point, the WiDirect is able to monitor and configure the access point. This page lists all the currently configured Access Points, as shown in Figure 1-31.

Adding access points to the system enhances future troubleshooting and configuration. For example, on Nortel networks it is very important to properly configure the Radius configuration files. By taking the time and entering all the AP information requested on this page, the WiDirect can use this information to assist during the Radius configuration step. For example, the WiDirect helps the administrator build Radius files based off the serial number of the Access Point. With other models of access points, such as the EnGenius ECB3500 and ECB9500, adding the access points allows the WiDirect to remotely configure the devices.

On the main access point page, administrators can edit or add new Access Points. By clicking on an Access Point, or clicking **Add New Access Point**, the **Access Point Edit** page will be displayed as shown in Figure 1-31. Table 1-8 describes all the possible values for this page.

Keyword	Description
MAC	The MAC address of the AP. This must be unique across all access points. The MAC can frequently be obtained from a sticker on the AP. **REQUIRED**
IP	The IP that the system will use to ping the AP, such as 10.3.1.50. This field must be

	filled in with a valid IP address for monitoring and data collection. **REQUIRED**
Alternate IP	This optional field is used to specify a secondary IP address for the access point. When using Tropos access points this field is required for any access points that are connected directly to the WiDirect.
Type	Sets the device type. Choices: Nortel, Proxim, Tropos, BelAir, EnGenius, Bridge, Other. Some access points have an automatic configuration option as well. If that option is chosen the WiDirect will automatically configure the access point. If the type is set to Bridge then the device will be displayed on the **Bridge Status** page, otherwise it will be displayed on the **AP Status** page.
Name	A descriptive name of the AP. This field should be kept relatively short (10-20 characters), because it is used in the TL graphing pages and visual management components. **REQUIRED**
Location	A description of the AP, used only on the configuration page.
Contact Info	Email address of the user who should be emailed on an up/down event. If no email address is defined, no email will be sent on up/down events.
Serial Num	The access point's serial number. For Nortel access points, the serial number is required to generate the keys in the radius file. For EnGenius access points this setting is used for automatic configuration. **REQUIRED**
SNMP	The SNMP public community string. If unsure, use the default of "public".
Latitude	Location of the AP. Used only on the configuration page.
Longitude	Location of the AP. Used only on the configuration page.
Mode	This Field identifies the access point as being connected to network backhaul (@NAP) or as a standard meshing access point (SAP) **REQUIRED**
Status	Dropdown field for defining the operational status of an access point (enabled / disabled) If a device is 'disabled', then it will not be monitored by the WiDirect. **REQUIRED**
Username	This field tells the WiDirect the telnet/web username for the Access Point. The default Nortel username is 'admin'
Password	This field tells the WiDirect the telnet/web password for the Access Point. The default Nortel password is 'admin'. When editing an access point this field can be left blank for the password to remain the same.

Table 1-8: Keywords and Descriptions for Access Points

MAC	IP	Type	Name	Serial	Location	Contact	Snmp	Mode	Username	Create Date	
00:00:00:00:00:01	10.4.1.2	BELAIR	NAP	BA100		SUPPORT@ANNAPOLISWIRELESS.COM		ENABLED		WED JUN 1 09:35:53 2011	DELETE
00:00:00:00:00:02	10.4.1.3	BELAIR	SAP1	BA101		SUPPORT@ANNAPOLISWIRELESS.COM		ENABLED		WED JUN 1 09:35:37 2011	DELETE
00:00:00:00:00:03	10.4.1.4	BELAIR	SAP2	BA103		SUPPORT@ANNAPOLISWIRELESS.COM		ENABLED		WED JUN 1 09:36:33 2011	DELETE

Figure 1-31: Access Points

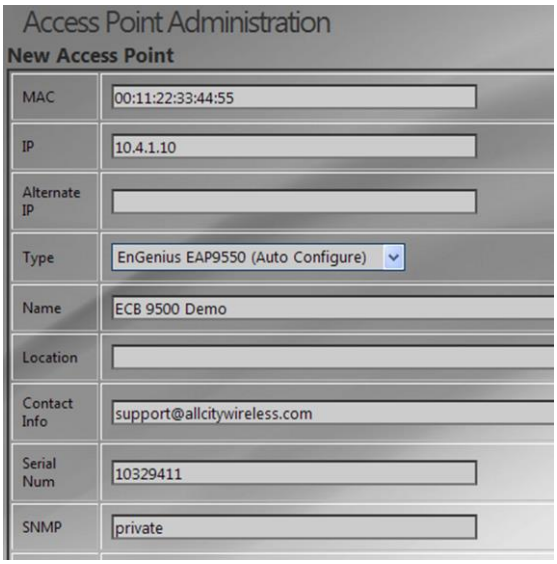


Figure 1-32: Adding a New Access Point

1.7.6 WiClients and WCMS

Each WiClient controls geographically separated networks over the Internet using WCMS. All user management is handled by the central WiDirect Authentication server, but the WiClient handles the process of redirecting the user to the central WiDirect when he or she first connects to the network. After a user is authenticated all their traffic goes straight from the WiClient to the Internet. If one WiClient goes down, only the people connected to that network are affected.

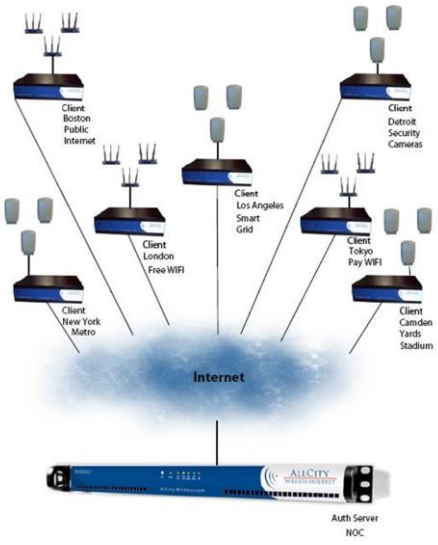


Figure 1-33: Example WiDirect Network

Figure 1-33 shows an example of a network with a WiDirect and WiClients at remote locations. Even though each of these clients lies on a separate network, they can all be setup to connect to the central WiDirect authentication server, which allows a common user base to be defined across all the wireless networks. To the user, all the WiDirect networks appear to be under a single entity.

To configure the list of WiDirect clients, click WiClients under the System Configuration menu. To add a new client, click the **Add a Client** link at the bottom of the ***WiClient Administration*** page. Table 1-9 lists all the fields for this page.

Keyword	Description
Description	The name of the WiDirect server. The built in "local" client is always named Local WiDirect.
Location	Text that describes the physical location of the WiDirect client.
Contact Info	Email address of the administrator that should be emailed when up/down events occurs for the client.
GWID	This is a unique identifier for each WiDirect. This field MUST be entered in correctly for WiDirect communication to occur. The GWID value is the MAC address of ETH1 interface without the colons. For example, if the MAC address of ETH1 was 00:00:0A:BC:DE:1F, the GWID value would be 00000ABCDE1F.
Status	Provides the enabled/disabled of the WiDirect.

Table 1-9: WiDirect Client Fields

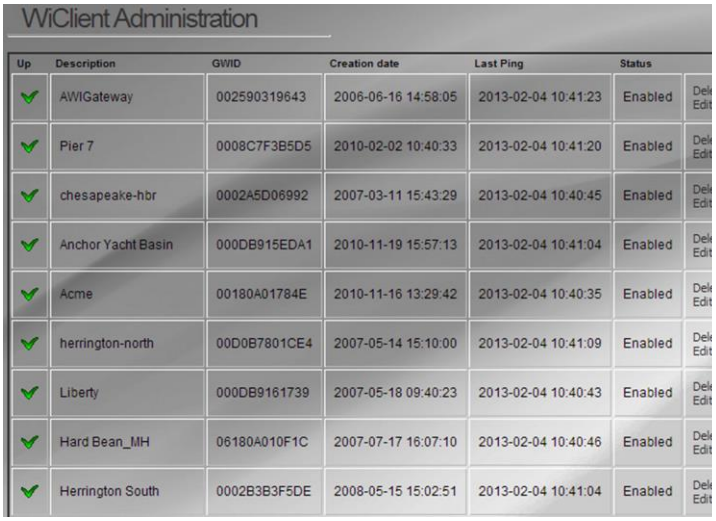


Figure 1-34: WiDirect Clients Page

1.7.7 Payment Gateways

The ***Payment Gateways*** page under the ***System Configuration*** menu allows for defining and managing payment gateways, such as PayPal or Authorize.net. Once at the **Payment Gateways** page, click **Add Payment Gateway** to add a new Payment Gateway.

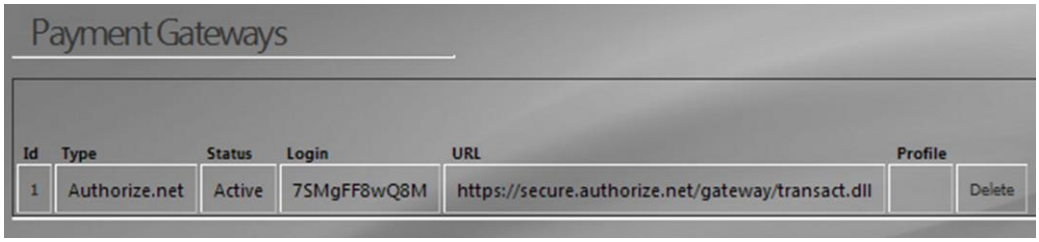


Figure 1-35: Payment Gateways

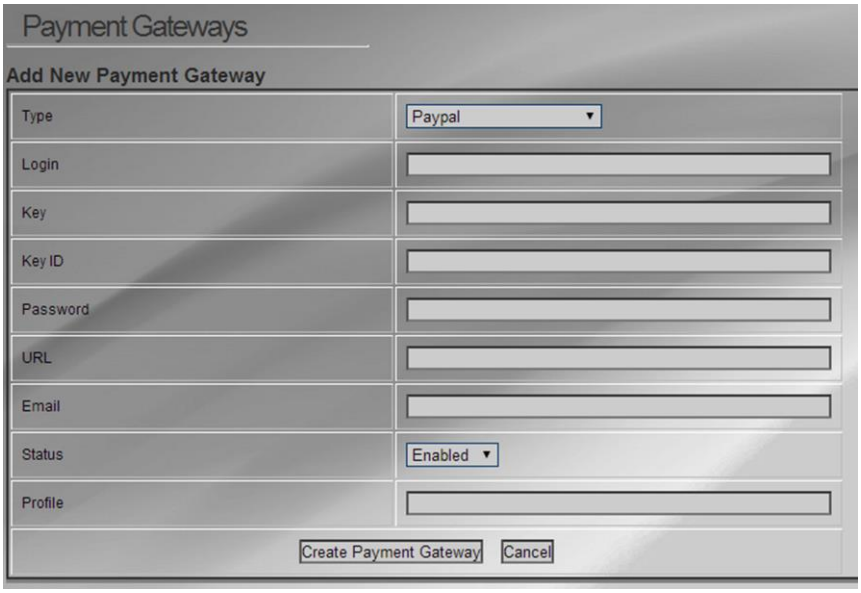


Figure 1-36: Adding Payment Gateway

From this page, first select the type of payment gateway desired, which is a drop down list next to the **Type** slot. Fill in the rest of the information, and click the **Create Payment Gateway** button at the bottom when finished. The different payment gateways have different requirements for the fields. For example, adding a payment gateway to handle coupons only requires the type, status, and profile fields to be set properly.

Administrators can also choose to look at the available Payment Gateways by the clicking on the **List All Payment Gateways** link at the bottom of the ***Payment Gateways*** page.

Keyword	**Description**
Type	Paypal, Authorize.Net, Authorize.net CIM, or Coupons. Defines which payment gateway to use.
Login	Authorize.net: API Login ID PayPal: Email address of the account GGe4 Hosted: Payment page ID GGe4 WiDirect: Password on Details page for Terminals
Key	Authorize.net: API login key GGe4 Hosted: Transaction key GGe4 WiDirect: HMAC key

Password	GGe4 WiDirect: Password on Details page for Terminals
URL	Authorize.net: https://secure.authorize.net/gateway/transact.dll. PayPal: https://www.paypal.com/cgi-bin/webscr. GGe4 WiDirect: https://api.globalgatewaye4.firstdata.com/transaction/v12 GGe4 Hosted: https://checkout.globalgatewaye4.firstdata.com/payment
Email	The email address of the account that is registered with the payment gateway.
Status	Enabled or Disabled. When a gateway is disabled, it will not be presented to the user as a payment option.
Profile	The profile that the payment plan is used. If this field is blank, the payment gateway will be available for all profiles.

Table 1-10: Fields for adding payment gateways.

Once the fields are all filled out, click **Create Payment Gateway** to activate this payment gateway.

Preferences Note:
In order for payments to work properly, the Validation Public Web IP option on the **Preferences** page must be set to the public IP or domain name of the WiDirect. The PayPal server makes a separate return call for each transaction to this IP address to report the successful payment. For Authorize.net payments this domain is used to redirect the user to a secure site to enter his or her payment information. The WiDirect should also have an SSL certificate installed to prevent the user from getting a certificate error.

Recurring Payments with Authorize.net CIM:
The WiDirect supports recurring payments using the Authorize.net CIM module. To setup recurring payments both an Authorize.net payment gateway and an Authorize.net CIM payment gateway need to be added on the WiDirect. The regular Authorize.net payment gateway should be disabled so that it does not appear on the purchase screen. It will be used internally for single one-time payments. If using recurring billing there must be only one Authorize.net payment gateway added, and one Authorize.net CIM payment gateway.

1.7.8 Network Configuration

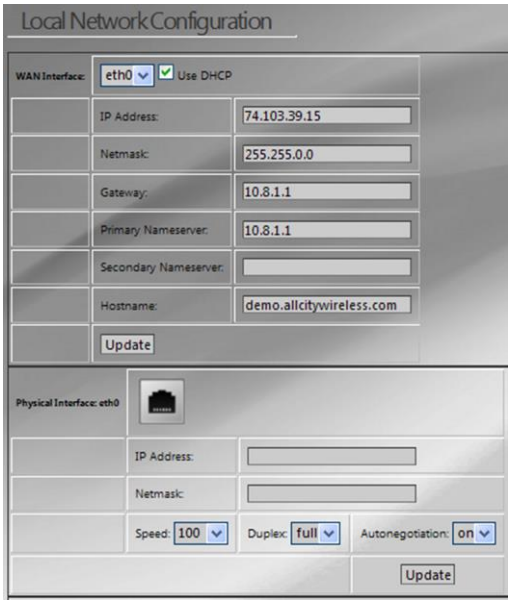


Figure 1-37: Network Configuration

Accurate IP address configuration is critical to the proper operation of the WiDirect. All network configuration and routing configuration is controlled via the ***Network Configuration*** page under the ***System Configuration*** menu. Figure 1-37 shows the **Network Configuration** window.

This page allows configuration of the WiDirect interfaces, the default route, and the DNS servers. The first section allows the administrator to set which interface is to be used as the WAN interface. By default the WAN interface is Eth0. If DHCP is enabled the Default Route and DNS server fields will be disabled, because that information will be retrieved via DHCP.

By default the Eth0 interface is configured for DHCP, and the Eth1 interface uses the standard 10.4.1.1 addressing scheme. IP addresses are not set by default for Eth2 or Eth3.

The bottom of the **Network Configuration** page has buttons to add a VLAN interface or a subinterface. A VLAN can be used on any interface to help separate users on the network. A subinterface is a secondary IP on the interface that will be on the same local network as the interface's main IP address. The pages to add a VLAN or Subinterface are shown in Figures 1-38 and 1-39. To add a VLAN or subinterface you must enter an IP address, netmask, and an ID number from 1 to 4095.

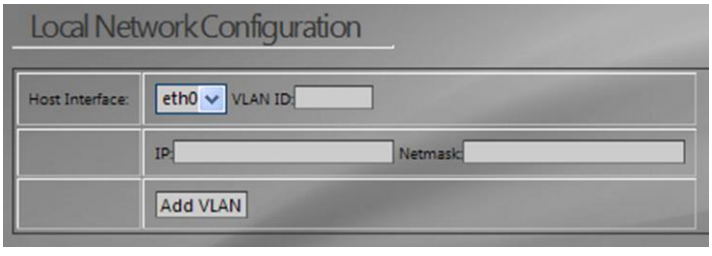


Figure 1-38: Create VLAN Interface

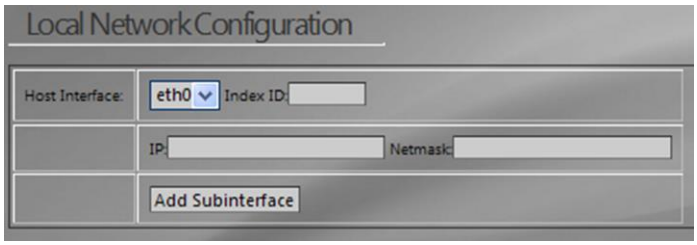


Figure 1-39: Create Subinterface

After the interfaces have been added they will show up on the ***Network Configuration*** page. From there the interfaces can either be updated or deleted.

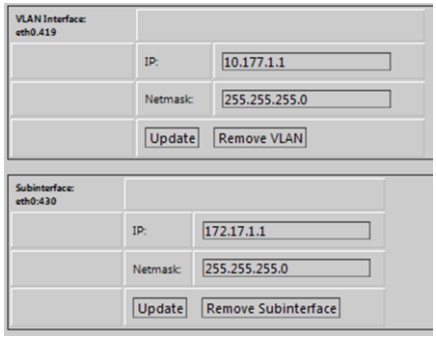


Figure 1-40: Network Configuration Page

1.7.9 Network Routing

Static routing can be configured via the administrative GUI interface in the ***Network Routing*** page under the ***System Configuration*** menu.

To add a route, simply click on **Add a Route** at the bottom of the screen. Fill in the information required and click the **Submit** button.

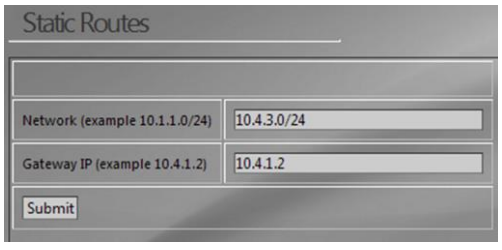


Figure 1-41: Network Routing Page

1.7.10 Date and Time

To modify the time settings select *Date and Time* under the System Configuration menu. From the drop down menus, set the time zone, date and time. Don't forget to click the **Update** button next to the appropriate commands to implement your selections. When making major changes to the time, or when changing the time zone, it is a good idea to restart the WiDirect. Refer to section 2 for a description of how to restart all system services without restarting the WiDirect.

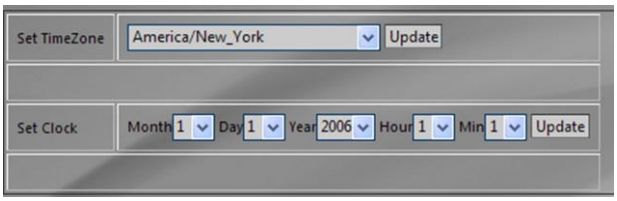


Figure 1-42: Date and Time

1.7.11 Log Viewer

With the ***Log Viewer*** page, located under the System Configuration menu, the log files can be viewed in real-time. Choose the appropriate log file by clicking on the link and a separate screen opens to view the log. This page will update as new entries are added to the log file. The purpose of each log file is described in Table 1-11.

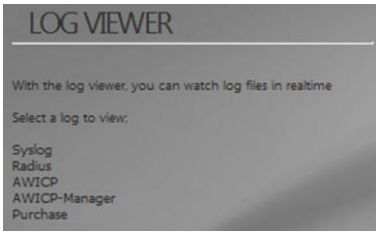


Figure 1-43: Log Viewer

Log File	Description
Syslog	This log file contains various system messages that can be helpful for troubleshooting problems. The log will contain a record of system events in case the WiDirect locks up. This file will also contain a record of DHCP requests, which can be helpful for troubleshooting a user who is having connection problems. When making changes to the DHCP configuration this log file can be helpful for identifying the source of any errors.
Radius	The Radius log file will contain a record of Radius messages that have been processed by the WiDirect.
AWICP	The AWICP log file is a record of log entries made by the captive portal. The log will contain a record of user logins and registrations, and may also include information if a user is having trouble signing on.
AWICP-Manager	The AWICP-Manager log file contains a record of users who are disconnected or have had their accounts expired by the WiDirect. This log will contain the reason that their account was disconnected or marked as expired.
Purchases	The purchases log file contains a record of users who have purchased access plans. It includes all Authorize.net and PayPal purchases.

Table 1-11: Descriptions of Log Files

1.7.12 License Key

The WiDirect comes preconfigured with a certain number of user licenses depending on the WiDirect model. There are two types of user classifications for licenses; **Active Users** and **Concurrent Users**. An Active User is a user that

has been registered and is eligible to use the network. All users, including users that have been disabled or expired, count towards the **Active User** count. **Concurrent Users** are the total number of users that can use the system simultaneously. Once the maximum number of concurrent users has been reached, new users must wait for a currently connected user to disconnect before using the network. All WiDirects shipping with version 1.5 and above have no restrictions on the number of concurrent users.

If needed, new license keys can be added to the WiDirect. To add new licenses, select ***License Key*** under the ***System Configuration*** menu. Browse to the directory where the license file is located on the local machine and then click **Upload**. The WiDirect will add the new license files to the database and the end user counts will be reflected in the license key tab.

Depending on usage of the system and the license that was originally purchased, a new license may need to be purchased to support more users. Contact support at AllCity Wireless if a new license is required.

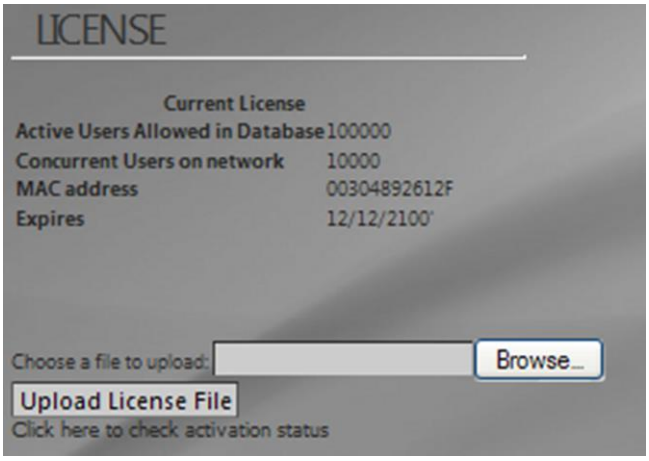


Figure 1-44: License Key

1.7.13 Admin Users

The ***Admin Users*** page allows the administrator to add and remove administrative accounts, change access levels, contact information, or even reset passwords.

Opening ***Admin Users*** under the ***System Configuration*** menu shows the list of administrators for the WiDirect device. Each administrator is assigned a user level that defines his/her access restrictions. Each administrator can have full (Administrator) or restricted (Report and Status Only) access to the administrative areas within the WiDirect.

Figure 1-45: Admin Users

1.7.13.1 Add New Administrator

In the ***User Admin*** screen of the WiDirect (pictured above), click on **Add Admin User**.

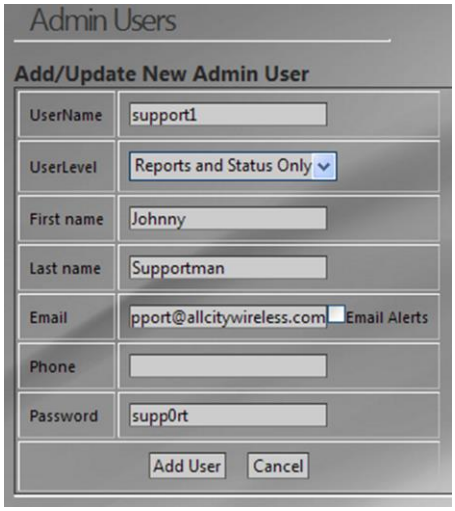


Figure 1-46: Add New Administrator

Fill in all the fields and click the **Add User** button. All fields should be self explanatory with the exception of User Level, which is described in the next section. If the email alerts box is checked then the administrator will get email alerts for certain events, such as for process restarts, low disk space alerts, and when a WiDirect is approaching its user license limit.

1.7.13.2 Change User Level

The customer can change any Administrator's role by selecting the desired new role from the drop down menu after clicking on the user's name and going into their profile. There are two user levels; ***Administrator*** and ***Reports & Status Only***. An ***Administrator*** level user has complete and total access to the WiDirect GUI system. A ***Reports & Status*** user can only view/edit WiDirect users, run status checks, and reports. The ***Reports & Status*** level user is a good setting for phone support staff.

1.7.13.3 Change Password

Each Administrator has a password that allows him or her access to the management console. To change the Administrator's password, enter the new password in the text box then click on the **Submit** button. A full access Administrator can change other administrator's passwords.

1.7.13.4 Delete

Select this button if you want to delete an administrator.

WARNING: **Never delete the admin user.** Instead change the password to something unique and keep it in a safe location. All administrators should have their own unique usernames and passwords.

1.7.14 SmartEdge

This page controls various settings for configuring the WiDirect to authenticate users on a SmartEdge. See section 4.21 for more details about the changes required to integrate with a SmartEdge. The configuration screen requires a forward policy (example "in: captiveportal"), a shared secret, the IP address of the WiDirect, and the IP address of the SmartEdge.

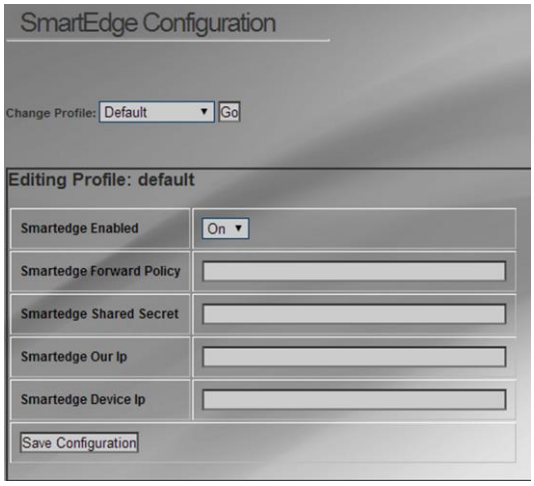


Figure 1-47: SmartEdge Configuration Screen

1.7.15 UAM

The UAM page allows for configuration of the UAM secret value. This option should correspond to the UAM secret value on the access point. For more details on UAM configuration see section 4.22.

1.7.16 Shutdown

The ***Shutdown*** page, which is listed under the ***System Configuration*** menu, allows the administrator to remotely shutdown or reboot the WiDirect unit. The appliance should never be powered off by disconnecting the power supply.

The shutdown procedure should be run to make sure that the file systems are correctly unmounted. If the WiDirect is not properly shutdown, it will cause a longer startup sequence the next time the WiDirect is powered up.

WARNING: Use this function with caution. Once the WiDirect unit is remotely shutdown, it can not be restarted unless someone has physical access to it.

1.7.17 Support

The ***Support*** page under the ***System Configuration*** menu displays the contact information you can use to contact a WiDirect professional in case you have additional questions. (Contact information is also listed at the end of this Manual.)

1.8 *Services Menu*

1.8.1 DHCP

The WiDirect provides DHCP services to all available LAN interfaces. Multiple subnets may be defined for each LAN interface, and each subnet has a definable DHCP lease address range associated with it. DHCP can be disabled on some subnets and enabled on others. Providing DHCP services on multiple subnets makes network administration easier because static addressing is not required on either subnet. DHCP can be configured to assign a given hardware Ethernet address (MAC) the same IP every time.

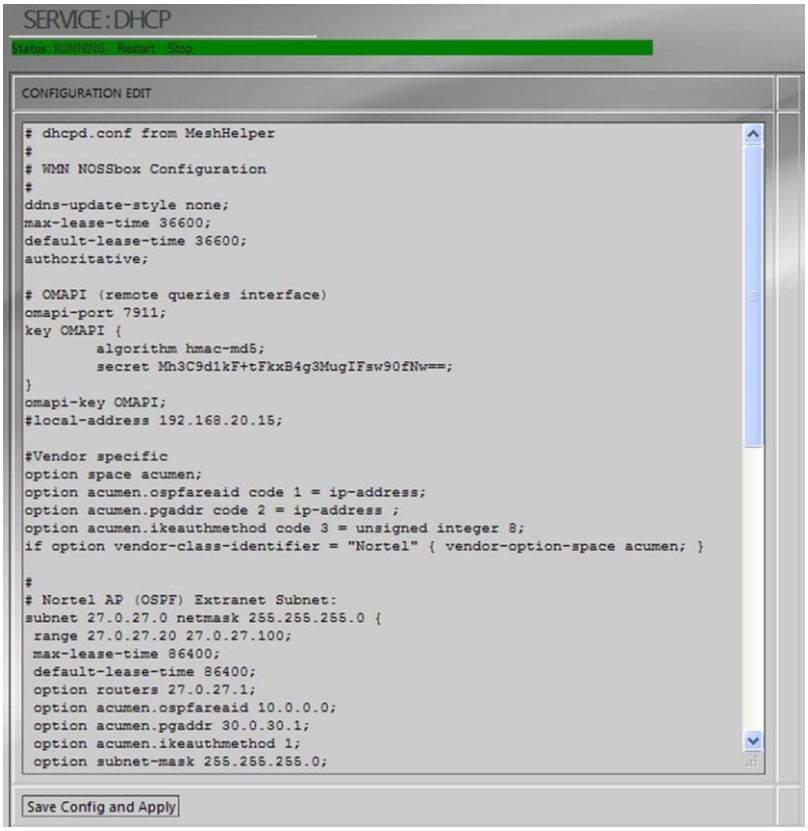


Figure 1-48: DHCP Service

To Edit the DHCP table click on ***DHCP*** under the ***Services*** menu. The entire DHCP configuration file will be presented in an editable text field, as shown in Figure 1-48.

Once the configuration has changed, use the **Save Config and Apply** to save the changes. This button is shown in Figure 1-49. The WiDirect automatically stores a retrievable backup of the file.

The WiDirect uses a standard version of DHCP that can be modified to suit any network environment. To learn about all the configuration items for this file, consult the ISC DHCP documentation at: *http://www.isc.org/products/DHCPD*

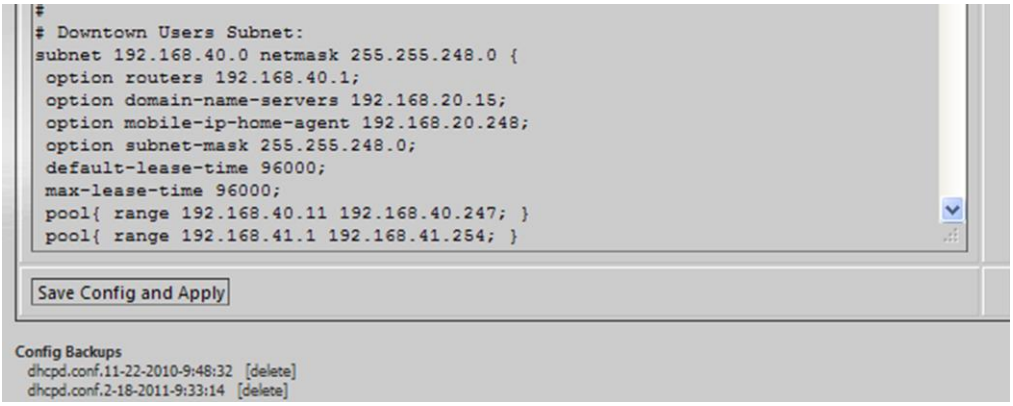


Figure 1-49: DHCP 'Save Config and Apply' Button

1.8.2 Radius

To generate Radius files for Nortel Access Points, go to the ***Services*** menu and click on ***Radius***, which opens the Radius configuration window as shown in Figure 1-50.

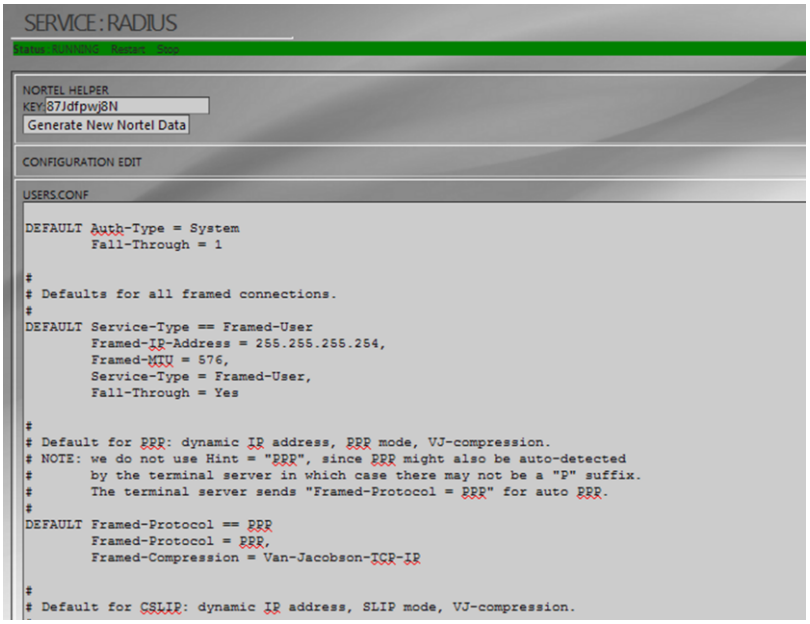

SERVICE : RADIUS
Status : RUNNING Restart Stop
NORTEL HELPER
KEY 87Jdfpwj8N
Generate New Nortel Data
CONFIGURATION EDIT
USERS.CONF
DEFAULT Auth-Type = System
Fall-Through = 1
#
Defaults for all framed connections.
#
DEFAULT Service-Type == Framed-User
Framed-IP-Address = 255.255.255.254,
Framed-MTU = 576,
Service-Type = Framed-User,
Fall-Through = Yes
#
Default for PPP: dynamic IP address, PPP mode, VJ-compression.
NOTE: we do not use Hint = "PPP", since PPP might also be auto-detected
by the terminal server in which case there may not be a "P" suffix.
The terminal server sends "Framed-Protocol = PPP" for auto PPP.
#
DEFAULT Framed-Protocol == PPP
Framed-Protocol = PPP,
Framed-Compression = Van-Jacobson-TCP-IP
#
Default for CSLIP: dynamic IP address, SLIP mode, VJ-compression.

Figure 1-50: Configuring Radius

The only two Radius files that are editable through the GUI are users and clients files. For most deployments, these files will not need to be edited. Please contact AllCity Wireless support or check the WiDirect web site for more information about special deployment options.

1.8.3 HTTP

To add an HTTP key or Certificate, go to the ***Services*** menu and click ***HTTP***. This page allows an administrator to configure a proper SSL certificate for the WiDirect.

While this page also has a **Restart** button at the top, which allows the HTTP service to be restarted, there are no **Stop** or **Start** buttons on this page. If the HTTP process was ever stopped, access to the Admin and user login pages would be impossible without a reboot of the WiDirect.

To update the certificates, simply cut and paste them into the **Key** and **Certificate** form fields and click **Update**. If there is an error with the new key and certificate, the old key and certificate will be automatically used instead. The new key and certificate installation should be verified in a web browser after updating.

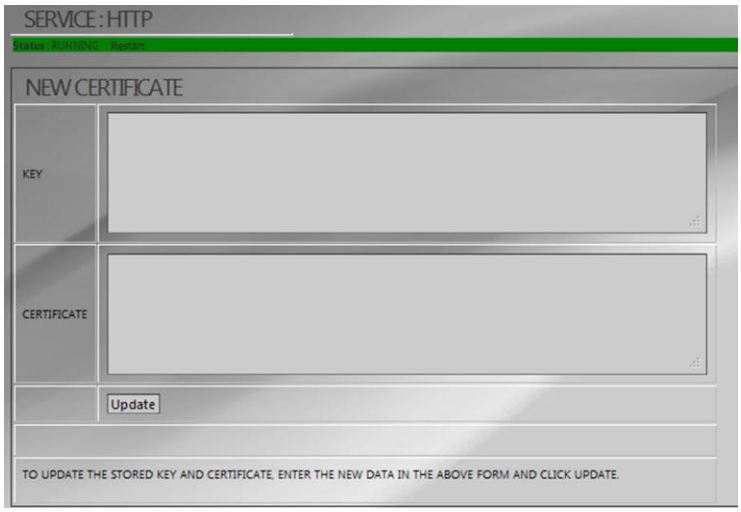

SERVICE : HTTP
Status : RUNNING Restart
NEW CERTIFICATE
KEY
CERTIFICATE
Update
TO UPDATE THE STORED KEY AND CERTIFICATE, ENTER THE NEW DATA IN THE ABOVE FORM AND CLICK UPDATE.

Figure 1-52: HTTP Management

1.8.4 Firewall

The firewall filters traffic that is passing between the LAN and WAN sides of the WiDirect. Firewalls can be programmed to block traffic based on a wide variety of criteria. Traditionally, firewalls enforce policies to maintain network security by using a set of rules that determine whether or not traffic is allowed to pass between the LAN and the WAN on a per-packet basis.

The Firewall configuration file also handles how certain user information is obtained from various services such as the user's MAC address, IP address, and Access Point. All of these settings are discussed in Tables 1-12 and 1-13.

The following section describes all the possible items for the Firewall configuration file. The first section describes all the Non-filtering firewall configuration items and the second section describes the traffic filtering configuration times. Firewall filtering rules dictate which traffic is allowed inbound and outbound of the WiDirect.

Hint: In the configuration file itself, there are commented lines which provide in-line configuration help. These lines begin with the pound (#) sign. Comments can be added to if needed by the Administrator.

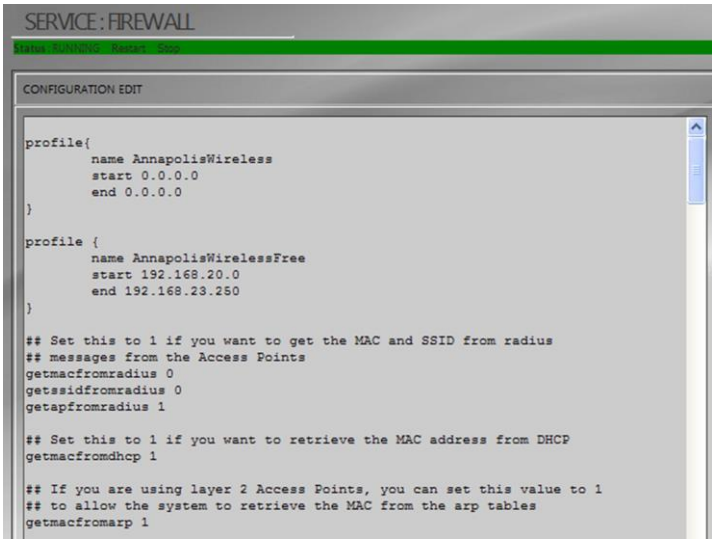

SERVICE : FIREWALL
CONFIGURATION EDIT
profile{
name AnnapolisWireless
start 0.0.0.0
end 0.0.0.0
}
profile {
name AnnapolisWirelessFree
start 192.168.20.0
end 192.168.23.250
}
Set this to 1 if you want to get the MAC and SSID from radius
messages from the Access Points
getmacfromradius 0
getssidfromradius 0
getapfromradius 1
Set this to 1 if you want to retrieve the MAC address from DHCP
getmacfromdhcp 1
If you are using layer 2 Access Points, you can set this value to 1
to allow the system to retrieve the MAC from the arp tables
getmacfromarp 1

Figure 1-53: Firewall Configuration Page

1.8.4.1 Firewall Configuration Options

Table 1-12 lists many of the firewall configuration items, such as how to obtain the Profile, AP, IP, and MAC addresses of users, how to turn on/off web caching, and how to add trusted users. The traffic filtering features are covered in the next section.

Keyword	Description

profile	Defines a profile, along with the IP address range assigned to that profile. This command saves processing time by eliminating the need to obtain the profile from Radius accounting messages, and is also available when the access point model does not support Radius messages. The default profile is set by setting the start and end IP range to 0.0.0.0. Example:
	profile {
	name AnnapolisWireless
	start 0.0.0.0
	end 0.0.0.0
	}

getapfromradius	Tells the WiDirect to obtain the user's Access Point information from the Radius Accounting messages. This option can also be used to obtain the information from DHCP relay requests if the domacauthfromdhcpd option is enabled.
getmacfromradius	Tells the WiDirect to obtain the user's MAC address from the Radius Accounting messages. This command should only be used if the standard

	DHCPD configuration is unavailable (See dhcpdommapi keywords below).
getssidfromradius	Tells the WiDirect to obtain the profile from the Radius Accounting messages. Should only be used if multiple profiles are configured on the network.
getapfromdhcp	Set this option to 1 for the WiDirect to get the MAC address of the access point from the DHCP server. This option requires DHCP relay to be enabled on the access point.
getmacfromdhcp	Tells the WiDirect to obtain the user's MAC address directly from the DHCP server. In almost all configurations, this command is the preferred over **getmacfromradius** because of increased speed and reliability.
dhcpdomapikey **dhcpdomapisecret** **dhcpdommapiserver**	These keywords are for DHCP communication when using the getmacfromdhcp command. If the standard configuration is used on the WiDirect for DHCP service, these commands should not change. If another DHCPD server is required, then these commands will need to change to point to the other DHCPD server and the new server will need to be configured for OMAPI. See the dhcpd.conf file for more information.
domacauthfromdhcpd	Set this option to 1 to allow for MAC authentication from DHCP. The DHCP service needs to be restarted after changing this option. For best performance in large networks this option should be disabled.
sociallogin-disabled	Set this option to 0 to allow for logins with social media accounts.
facebook-permit-time **google-permit-time** **linkedin-permit-time**	These options control how long the user has to authenticate with the corresponding social networking site after clicking the initial login button. The time should be entered in seconds. If not set then they default to 300 seconds.
TrustedIPList	This command allows the WiDirect to allow a set of trusted IP addresses from the internal side of the network to the Internet without Captive Portal challenge. The IP addresses should all appear on a single line, separated by commas. Multiple TrustedIPList lines are allowed in the configuration file. Example: **TrustedIPList 192.168.20.11,10.4.1.20,10.4.1.30**
TrustedMACList	This command allows the administrator to enter a list of trusted MAC addresses. These devices will be allowed direct Internet access without any restrictions. Multiple TrustedMACList lines are allowed in the configuration file.
preproxy	Preproxy must be enabled to use the walled garden or landing page feature. Set preproxy to 0 to disable these features.
applesupport	Set this value to 1 to have older Apple mobile devices, such as the iPhone and iPad, automatically display the login page when the device connects to the WiFi network. If the device doesn't login then it will automatically disconnect from the network.
landingpage	The landing page is the page the user is redirected to when they start using the network. If the landing page is not specified, then the user will be redirected to the login page. The landing page needs to contain a link to the login page for the user to be able to login. When updating the landing page, the PreProxy service also needs to be restarted from the PreProxy service page.

postproxy	Postproxy is used to handle web caching, acceleration, monitoring, and content filtering. Set this value to 0 to disable the web proxy for all users. Set this value to 1 to enable the web proxy for all users. Setting this value to 2 will enable the web proxy only for users on an access plan with content filtering or interstitial advertisements enabled.
HostName **SSLAvailable**	If the WiDirect has a valid certificate installed, then the HostName should be set appropriately, and SSLAvailable should be set to yes. This enables the login page to be accessed securely. In a **WiDirect Client** the HostName option should be set to the hostname of the main WiDirect server.
GatewayInterface	The gateway interface is the interface that users are forced to authenticate on. By default only eth1 is listed as a gateway interface. To authenticate users on additional interfaces you can have multiple GatewayInterface lines.
ChekInterval	The time (seconds) interval between the regular periodic updates between the WiClient and WiDirect.
authdowncount	The maximum number of WiDirect ping failures (pinged every CheckInterval seconds) until the currently active WiDirect is considered down and when the WiClient switches over to the next WiDirect server (if available).
authdownaction	Controls what type of Internet access users of the WiClient are given while all the WiDirect servers are considered down (have reached 'authdowncount'). **restricted** The default. Only the people already authenticated are allowed access to the Internet. **permit** Allow all users access while the AuthServer(s) are down. **deny** All users are denied access to the Internet while the AuthServer(s) are down.

Table 1-12: Firewall Configuration Items

1.8.4.2 Traffic Filtering Firewall Configuration Items

The firewall rules are broken into two **RuleSets**; **Global** & K**nown-users**. While there are other defined RuleSets in the firewall configuration file, editing is NOT supported at this time. AllCity Wireless only supports the Global and Known-users Rulesets at this time.

Firewall Syntax

Essentially, there are allow and block rules. These rules are processed in FIFO (first in, first out) order, which means the first match wins. Here is an example of firewall rules.

```
firewall allow tcp port 80 to 10.10.1.1
firewall allow udp to 172.32.1.0/24
firewall block to 172.16.0.0/12
```

Syntax of the Firewall command is as follows:

FirewallRule *action* [tcp | udp] [port XYZ] [to IP][/subnet]

Table 1-13 describes each portion of this command in detail.

FirewallRule	Mandatory. Tells the WiDirect that the rule is a static firewall rule.

FirewallDynamicRule	Optional. May be used instead of FirewallRule. Tells the WiDirect that this firewall rule is dynamic, so the WiDirect will continually lookup the IP address of the domain specified. When the IP updates the firewall rule will be updated.
action	Describes the behavior of the line. It can be set as either *allow* or *block*.
tcp | udp	Optional. Describes what type of traffic to filter.
port XYZ	Optional. Describes a specific port to block or allow. Ports value XYZ can be a number from 1 to 65536.
to IP	Optional. Defines a specific IP or IP range to apply the rule. A domain is allowed here as well. If the domain points to multiple IPs, only the first IP address found will be used. Use a FirewallDynamicRule if the domain has multiple IP addresses.
/subnet	Optional. Can only be used with the IP command, which defines a subnet rather than a specific IP to apply the list to.

Table 1-13: FirewallRule Options

Global

The Global firewall section defines all the rules that apply to every single state of the user's connection. A user's state could be '**unknown**', '**known**', and '**disabled**'. Any global firewall rules that are defined will apply to all these states. In other words, if a rule is defined in the Global section that allows the users to access a certain IP address, all users are allowed to access that IP address even if they have not logged into the WiDirect's captive portal.

A good example is allowing users to access advertisement driven sites without logging into the system, which provides a different sort of walled garden definition. In some cases, some ad insertion sites only need access to certain IP address instead of an entire domain. If requirements state that certain ads are displayed on the user's login page, this section might be the only way to provide access to the image and links on the login page.

Another instance when users need to be allowed to access certain IP addresses is for PayPal support. Users must be able to login to their PayPal account to pay for their access plan, so port 443 for the IP addresses of the PayPal web site must be allowed in the firewall. Due to the nature of the secure http protocol, walled garden sites can only use regular non-secure http.

Known-users

The Known-users firewall section defines firewall rules for users that have successfully authenticated to the WiDirect. Although it might seem counter intuitive, this section allows an Administrator to deny traffic to specific destinations. By default, the WiDirect allows authenticated users to have complete unrestricted access to the Internet with the following RuleSet:

```
FirewallRuleSet known-users {
   FirewallRule allow to 0.0.0.0/0
}
```

For example, if requirements state that users are not allowed to access SMTP to any mail server except the local SMTP relay with an IP address of 10.1.1.10, the configuration might look like this:

```
FirewallRuleSet known-users {
        # Allow SMTP to our SMTP relay
        FirewallRule allow tcp port 25 to 10.1.1.100
        # Deny all other SMTP traffic
        FirewallRule block tcp port 25
        #
        # Now just let every out everywhere (required rule)
        FirewallRule allow to 0.0.0.0/0
}
```

1.8.5 NTP

The WiDirect appliance internal clock must remain accurate for a number of the critical systems to function. In order to make this work properly, an NTP server is polled to synchronize the internal clock with a known NTP clock. NTP also provides time services to local devices.

To edit the NTP configuration, go to the ***NTP*** page under the ***Services*** menu. This is the standard NTP configuration and it will allow you to change NTPD servers as needed. If more information is required for configuring NTP, please see the NTP web site: http:://www.ntp.org.

NOTE: This page is NOT where you change the local date and time, this is only for Network Time Protocol (NTP). To configure the Date & Time on the WiDirect, see the **Date and Time Configuration** section in this document.

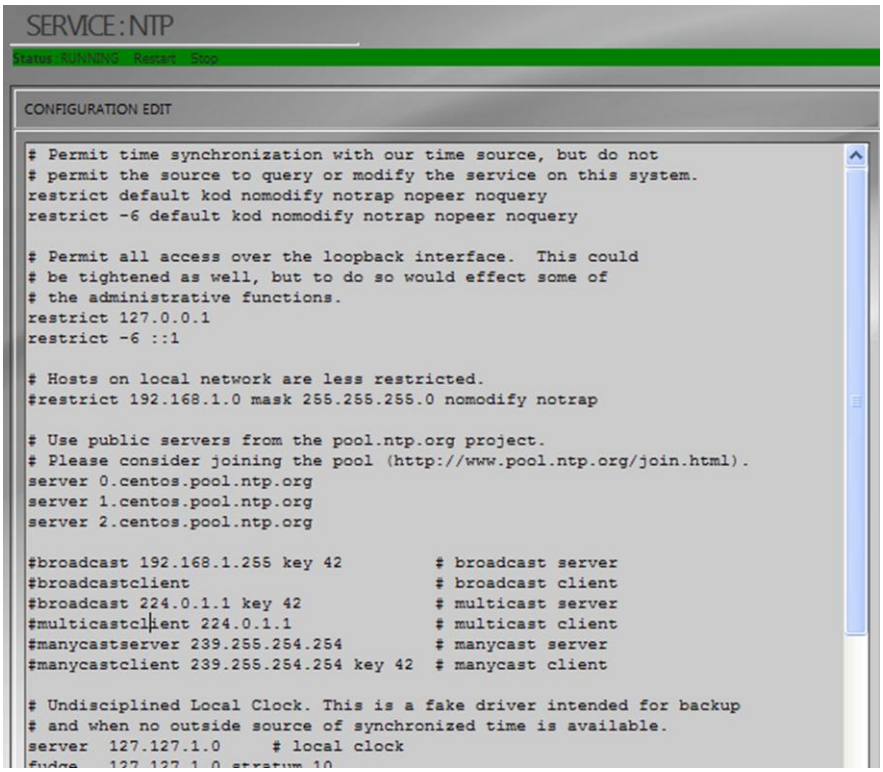

SERVICE : NTP
Status : RUNNING Restart Stop
CONFIGURATION EDIT
Permit time synchronization with our time source, but do not
permit the source to query or modify the service on this system.
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery
Permit all access over the loopback interface. This could
be tightened as well, but to do so would effect some of
the administrative functions.
restrict 127.0.0.1
restrict -6 ::1
Hosts on local network are less restricted.
#restrict 192.168.1.0 mask 255.255.255.0 nomodify notrap
Use public servers from the pool.ntp.org project.
Please consider joining the pool (http://www.pool.ntp.org/join.html).
server 0.centos.pool.ntp.org
server 1.centos.pool.ntp.org
server 2.centos.pool.ntp.org
#broadcast 192.168.1.255 key 42 # broadcast server
#broadcastclient # broadcast client
#broadcast 224.0.1.1 key 42 # multicast server
#multicastclient 224.0.1.1 # multicast client
#manycastserver 239.255.254.254 # manycast server
#manycastclient 239.255.254.254 key 42 # manycast client
Undisciplined Local Clock. This is a fake driver intended for backup
and when no outside source of synchronized time is available.
server 127.127.1.0 # local clock

Figure 1-54: NTPD Configuration

1.8.6 Preproxy

When enabled in the firewall configuration file, the Preproxy service is responsible for redirecting users to either the login page or to the landing page. It also allows users to visit sites on the walled garden without logging in. The configuration file may be edited to change the number of processes that are running at any given time. Typically the default settings are fine. In a large network, or if a lot of users are going to use the walled garden functionality, it is a good idea to increase the number of Preproxy processes.

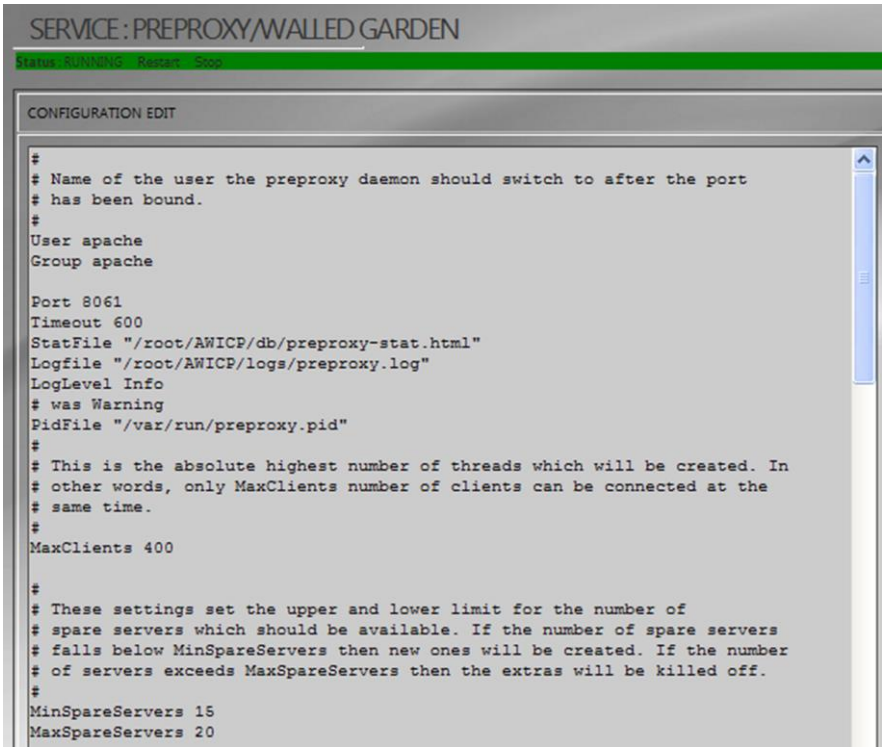

SERVICE : PREPROXY/WALLED GARDEN
Status: RUNNING Restart Stop
CONFIGURATION EDIT
#
Name of the user the preproxy daemon should switch to after the port
has been bound.
#
User apache
Group apache
Port 8061
Timeout 600
StatFile "/root/AWICP/db/preproxy-stat.html"
Logfile "/root/AWICP/logs/preproxy.log"
LogLevel Info
was Warning
PidFile "/var/run/preproxy.pid"
#
This is the absolute highest number of threads which will be created. In
other words, only MaxClients number of clients can be connected at the
same time.
#
MaxClients 400
#
These settings set the upper and lower limit for the number of
spare servers which should be available. If the number of spare servers
falls below MinSpareServers then new ones will be created. If the number
of servers exceeds MaxSpareServers then the extras will be killed off.
#
MinSpareServers 15
MaxSpareServers 20

Figure 1-55: Preproxy Configuration

1.8.7 Web Cache

When enabled in the firewall configuration file, the web caching service is responsible for accelerating user's web sites, tracking sites visited, content filtering, and advertisement delivery.

1.8.8 DNS

The DNS configuration page allows you to configure the DNS server. The default DNS configuration for older WiDirects only listens for DNS requests on eth1, eth2, and eth3. Newer WiDirects will listen on all interfaces except eth0 for DNS requests. If VLANs have been added then the configuration should be checked to make sure interfaces are responding to DNS requests as appropriate.

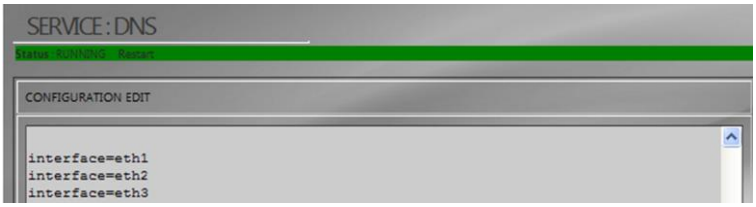


Figure 1-56: DNS Configuration

Figure 1-56 shows the part of the DNS file that needs to be edited to add additional interfaces. Each interface is listed on its own line. VLAN interfaces would be a combination of the VLAN tag number and the interface name. VLAN 600 on eth1 would be listed as eth1.600. To listen on all interfaces simply remove or comment out all the interface lines. DNS requests on eth0 will still be blocked by the firewall, so additional configuration is required to listen for DNS requests on eth0.

1.9 Access Point Support

1.9.1 Ericsson

1.9.1.1 Access Point Configuration

The **BelAir Configuration** page allows you to configure various settings on the BA100 and BA200 access points. For the WiDirect to control these access points they need to be added to the access point database with the correct Ethernet MAC addresses and serial numbers. The type should be set to "BelAir 100 Auto Configure" or "BelAir 200 Auto Configure." The **BelAir Configuration** link will bring you to a page where you the administrator decide which radios to configure. There are different configuration pages for the BA100 and BA200 access points, as well as different configuration pages for each of the individual radios.

Figure 1-57: AP and Radio Selection

After selecting the access point model and radio to configure, an additional page will be displayed allowing you to set configuration items for that radio. Both access and backhaul configuration changes can be made. After the changes are made a confirmation message, along with any error messages, will be placed in the Event Viewer. It will take the WiDirect approximately five minutes per access point before the devices are automatically configured.

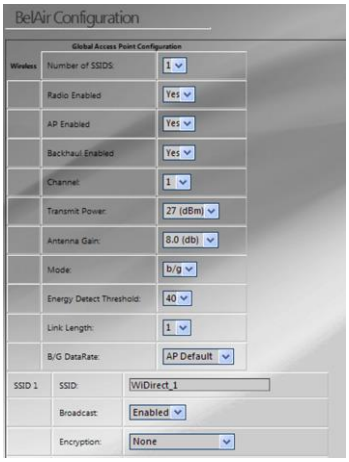


Figure 1-58: BelAir Configuration Page

1.10 Tools

The **Tools** section provides the WiDirect administrator with the basic network troubleshooting tools of ping, trace route, and DNS query.

1.10.1 Ping

Ping allows an administrator to test network connectivity by sending a ping request to another machine on the network. Enter in the target IP address of the remote machine to test and click the **Ping** button. The results of the ping will be displayed.

This example is a successful ping of IP 192.168.20.248:

PING 192.168.20.248 (192.168.20.248) 56(84) bytes of data.
64 bytes from 192.168.20.248: icmp_seq=1 ttl=64 time=0.310 ms
64 bytes from 192.168.20.248: icmp_seq=2 ttl=64 time=0.264 ms
64 bytes from 192.168.20.248: icmp_seq=3 ttl=64 time=0.214 ms
--- 192.168.20.248 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.214/0.262/0.310/0.043 ms

1.10.2 Traceroute

Like the **Ping** command, the **Traceroute** command tests network connectivity by attempting to find the network path between the WiDirect and another network device. Type in the target address and click the **Traceroute** button. The results of the **Traceroute** will be displayed after the WiDirect executes the command.

Example output:

traceroute to 10.3.1.50 (10.3.1.50), 30 hops max, 40 byte packets
1 balance (192.168.200.1) 1.875 ms 2.286 ms 2.747 ms
2 73.135.120.1 (73.135.120.1) 81.174 ms 93.181 ms 93.600 ms
3 ge-1-20-ur01.annapolis.md.bad.comcast.net (68.87.136.205) 94.065 ms 94.535 ms 94.514 ms
4 te-9-3-ur02.gambrills.md.bad.comcast.net (68.87.128.150) 94.983 ms 94.957 ms 96.891 ms
5 te-9-1-ur01.gambrills.md.bad.comcast.net (68.87.129.17) 94.858 ms 97.319 ms 97.295 ms
6 te-7-1-ar01.capitolhghts.md.bad.comcast.net (68.87.129.22) 97.265 ms 79.813 ms 80.194 ms
7 12.86.111.5 (12.86.111.5) 81.152 ms 117.899 ms 141.375 ms
8 tbr2.wswdc.ip.att.net (12.122.113.78) 162.803 ms 163.262 ms 163.726 ms
9 cr1.wswdc.ip.att.net (12.122.16.89) 164.194 ms 164.173 ms 164.619 ms
10 cr2.phlpa.ip.att.net (12.122.4.53) 165.089 ms 165.062 ms 165.504 ms
11 tbr2.phlpa.ip.att.net (12.122.20.86) 167.469 ms 167.444 ms 167.894 ms
12 tbr2.cgcil.ip.att.net (12.122.10.93) 166.859 ms 171.816 ms 172.279 ms
13 12.122.99.93 (12.122.99.93) 113.359 ms 105.891 ms 183.838 ms
14 12-215-4-17.client.mchsi.com (12.215.4.17) 321.209 ms 321.622 ms 321.111 ms
*15 12-215-8-163.client.mchsi.com (12.215.8.163) 328.543 ms * **
*16 10.3.1.50 (10.3.1.50) 338.253 ms 267.762 ms **

1.10.3 DNS Query

The ***DNS Query*** command allows an administrator to test DNS connectivity. DNS is very important because the captive portal uses it to detect a user's initial Internet request. DNS is also used in some services such as FTP.

For Domain resolution check, go to the ***Tools*** menu and then ***DNS Query***. Then type in a domain name to query, for example www.google.com, and click the ***Lookup*** button. The results will be displayed once the lookup completes.

DNS look up of www.google.com
Server: 192.168.200.1
Address: 192.168.200.1#53

Non-authoritative answer:
www.google.com canonical name = www.l.google.com.
Name: www.l.google.com
Address: 64.233.161.99
Name: www.l.google.com
Address: 64.233.161.104
Name: www.l.google.com
Address: 64.233.161.103
Name: www.l.google.com
Address: 64.233.161.147

1.11 Voucher Management Page

To get to the voucher management page click on "Open WiDirect Guest-Pass Manager" on the Voucher Administration Users page. Enter a valid username and password to access the voucher system.

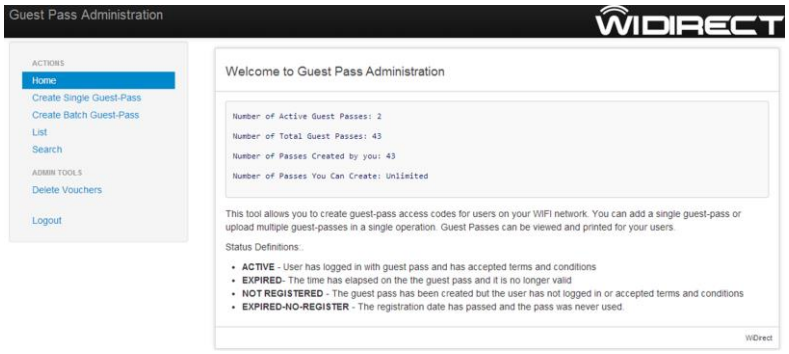

Guest Pass Administration
WIDIRECT
ACTIONS
Home
Create Single Guest-Pass
Create Batch Guest-Pass
List
Search
ADMIN TOOLS
Delete Vouchers
Logout
Welcome to Guest Pass Administration
Number of Active Guest Passes: 2
Number of Total Guest Passes: 43
Number of Passes Created by you: 43
Number of Passes You Can Create: Unlimited
This tool allows you to create guest-pass access codes for users on your WIFI network. You can add a single guest-pass or upload multiple guest-passes in a single operation. Guest Passes can be viewed and printed for your users.
Status Definitions:
ACTIVE - User has logged in with guest pass and has accepted terms and conditions
EXPIRED- The time has elapsed on the the guest pass and it is no longer valid
NOT REGISTERED - The guest pass has been created but the user has not logged in or accepted terms and conditions
EXPIRED-NO-REGISTER - The registration date has passed and the pass was never used.
WiDirect

Figure 1-59: Main Guest Pass Administration Page

1.11.1 Create Single Guest-Pass

Name, Email	Enter in any information about the user that will be using this voucher. This information will help lookup the account later.
Code	The code the user will enter to access the network. This value is filled in automatically, but can be modified.
Valid For	This option determines how long the voucher will be valid for after it has been activated. This value can be shorter than the plan setting, which will stop the user from accessing the network prior to the time their account would normally be active. This option allows for a single access plan with unlimited time to be used to

	create vouchers that are valid for varying lengths of time.
Plan	The access plan that a user created with this voucher will be placed on. If desired be sure the Valid For time is sufficient to allow the user to use the entire time alotted by their plan.
Date Must Register By	Specify the date that the user must use the voucher before it is no longer active.
Comments	Enter any additional comments regarding this voucher here.

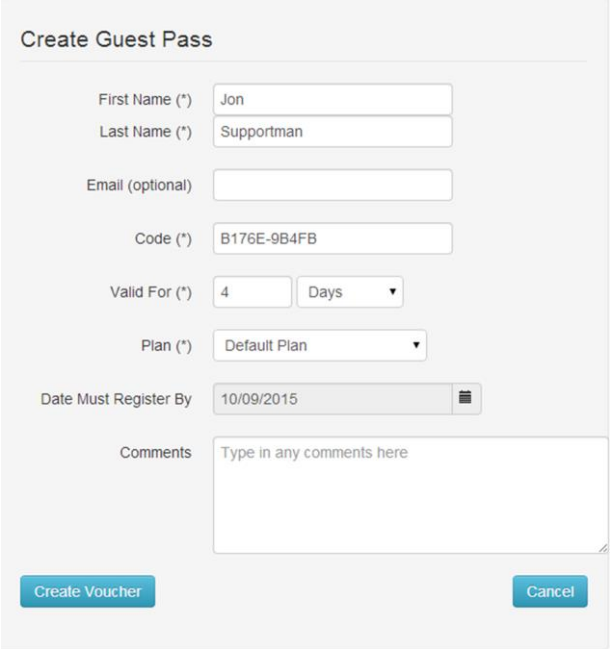


Figure 1-60: Create Single Voucher

1.11.2 Create Batch Guest-Pass

This page allows for the creation of multiple vouchers at the same time. For a description of the fields read the section on creating a single guest pass. The voucher codes will be generated automatically when creating multiple guest passes.

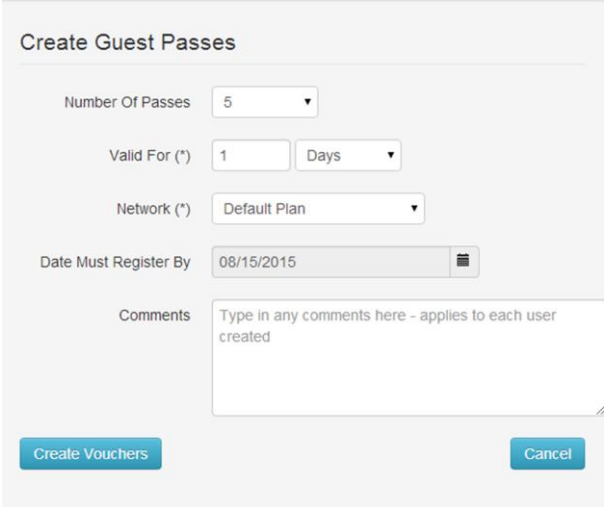


Figure 1-61: Main Guest Pass Administration Page

1.11.3 List

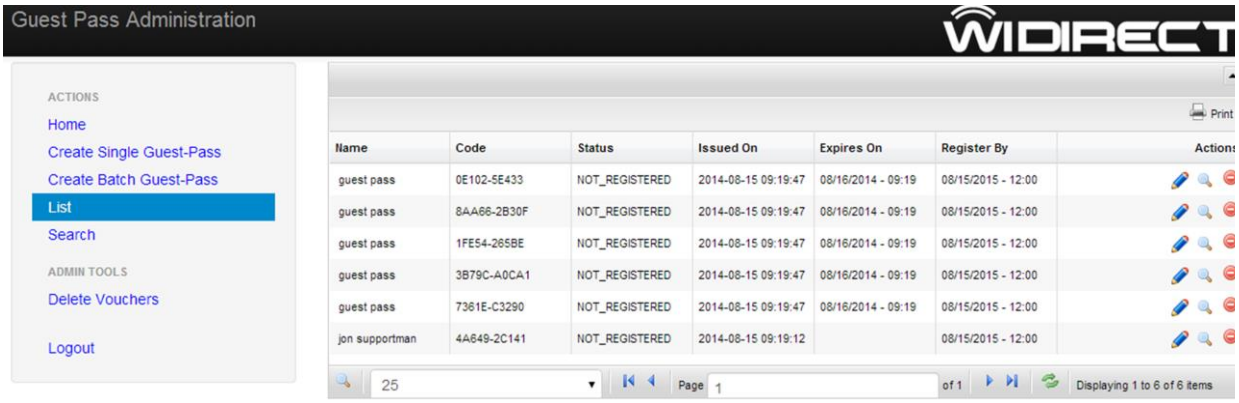

Guest Pass Administration
WIDIRECT
ACTIONS
Home
Create Single Guest-Pass
Create Batch Guest-Pass
List
Search
ADMIN TOOLS
Delete Vouchers
Logout
Print
Name
Code
Status
Issued On
Expires On
Register By
Actions
guest pass 0E102-5E433 NOT_REGISTERED 2014-08-15 09:19:47 08/16/2014 - 09:19 08/15/2015 - 12:00
guest pass 8AA66-2B30F NOT_REGISTERED 2014-08-15 09:19:47 08/16/2014 - 09:19 08/15/2015 - 12:00
guest pass 1FE54-265BE NOT_REGISTERED 2014-08-15 09:19:47 08/16/2014 - 09:19 08/15/2015 - 12:00
guest pass 3B79C-A0CA1 NOT_REGISTERED 2014-08-15 09:19:47 08/16/2014 - 09:19 08/15/2015 - 12:00
guest pass 7361E-C3290 NOT_REGISTERED 2014-08-15 09:19:47 08/16/2014 - 09:19 08/15/2015 - 12:00
jon supportman 4A649-2C141 NOT_REGISTERED 2014-08-15 09:19:12 08/15/2015 - 12:00
25
Page 1 of 1
Displaying 1 to 6 of 6 items

Figure 1-62: Main Guest Pass Administration Page

1.11.4 Search

On the Search page click on the magnifying glass on the bottom left of the table to bring up a field to enter a search string. Click the "Search" button to complete the search. Once a list of items comes up then similar to the List page there is the ability to delete or bring up the details about a voucher.

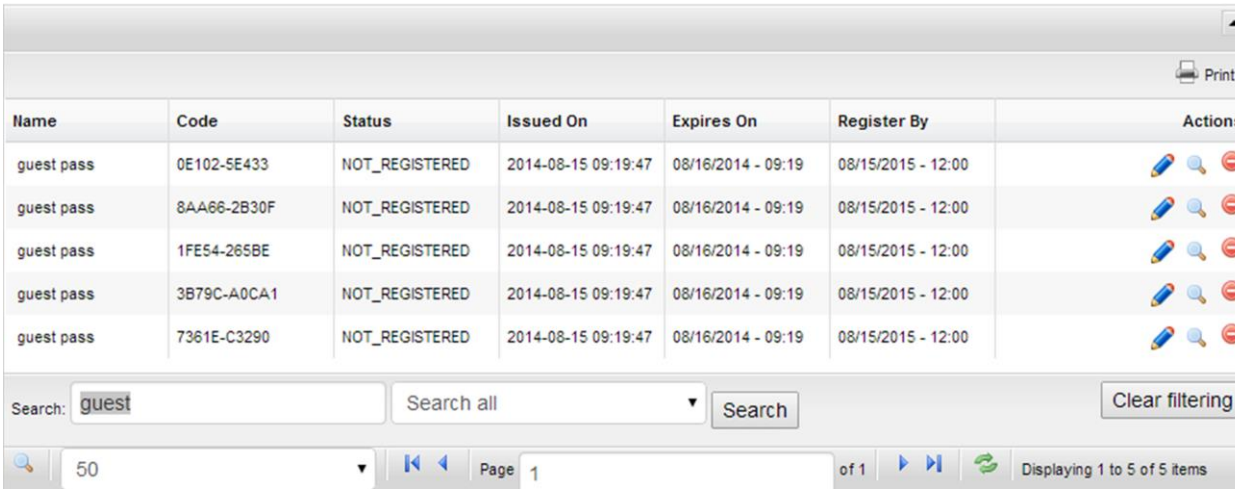

Print
Name
Code
Status
Issued On
Expires On
Register By
Actions
guest pass 0E102-5E433 NOT_REGISTERED 2014-08-15 09:19:47 08/16/2014 - 09:19 08/15/2015 - 12:00
guest pass 8AA66-2B30F NOT_REGISTERED 2014-08-15 09:19:47 08/16/2014 - 09:19 08/15/2015 - 12:00
guest pass 1FE54-265BE NOT_REGISTERED 2014-08-15 09:19:47 08/16/2014 - 09:19 08/15/2015 - 12:00
guest pass 3B79C-A0CA1 NOT_REGISTERED 2014-08-15 09:19:47 08/16/2014 - 09:19 08/15/2015 - 12:00
guest pass 7361E-C3290 NOT_REGISTERED 2014-08-15 09:19:47 08/16/2014 - 09:19 08/15/2015 - 12:00
Search: guest
Search all
Search
Clear filtering
50
Page 1 of 1
Displaying 1 to 5 of 5 items

Figure 1-63: Main Guest Pass Administration Page

1.11.5 Delete Vouchers

This page allows you to delete vouchers that are expired. It may be helpful to keep vouchers that users have registered with for the various reporting pages on the WiDirect.

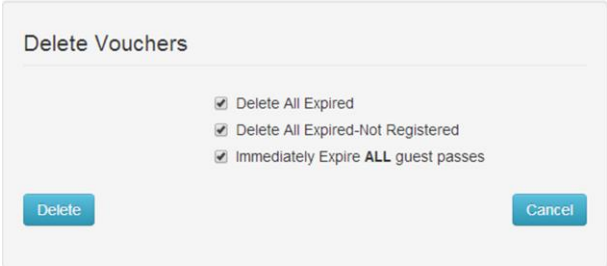


Figure 1-64: Delete Vouchers Page

2 Command Line Interface

2.1 Secure Shell access

An SSH client is required in order to access the command line interface of the WiDirect. If you are using Windows, AllCity Wireless recommends using *putty* for SSH access, which is a free download at this website:

http://www.chiark.greenend.org.uk/~sgtatham/putty/

Other operating systems include an SSH client by default. After opening putty, or another SSH client, connect to the IP address of the WiDirect machine. By default this IP address is 10.4.1.1 on the ETH1 interface. However, if the IP address of any of the WiDirect's interface has changed, the new IP address should be the one that used in the SSH connection. If you are accessing from the Internet, you'll want to use the public IP address of the WiDirect.

Once connected, the system will ask for a login and password. For security reasons, the root username cannot be used. Administrators must use the **portal** login to gain access. The account **awisupport** is also available for SSH logins. If this is a new system, the password will be **widirect**. Since command line access gives full control over the WiDirect, including the ability to look up passwords to the web GUI, it is important that a secure password be set.

Once connected, administrators are free to use any of the standard Linux commands to navigate the system. To perform any advanced configuration changes we strongly suggest using the **sudo** command instead of switching to the root user. See the **sudo** section below for more information.

To exit the command line interface, use the **logout** command or **CONTROL-D**.

NOTE: If editing files, consult the VI quick reference guide located in this document.

2.2 Using sudo commands

For security reasons, the WiDirect allows the **portal** user to run the **sudo** process without switching to the root user, which allows root level access to various parts of the system. Only top-level Administrators should have the root password.

To use sudo, append the word **sudo** in front of any command. For example, to edit the iptables file, which is owned by root, use the following command.

sudo vi /etc/sysconfig/iptables

Sudo prompts for the **portal** password, not root password. This is done to verify that it's still the person that originally connected to the SSH process.

Sudo works for any commands that require root access.

2.3 Changing the password

It is a good idea to change the password of the portal user. When logged in as the portal user, use the passwd command and select a new secure password.

There is also an account that is used by the support staff to perform maintenance and monitor for problems. This password should be set by the support staff to something secure. To change the password on this account, execute the following command:

sudo passwd awisupport

2.4 Restarting System Services

When changing the IP address of ETH1 a full system restart can be avoided by simply restarting the WiDirect processes by using the following commands:

su -
/root/AWICP/bin/widirect_stop_all.sh
/root/AWICP/bin/widirect_start_all.sh
service dhcpd restart

The process of stopping and starting will take about 45 seconds. When changing the time zone some additional services need to be restarted in addition to the ones mentioned above:

sudo /sbin/service mysqld restart
sudo /sbin/service httpd restart

Restarting the access point monitoring processes can be done to get up to date data on the access points:

sudo /sbin/service awicp_ap_ping_monitor restart
sudo /sbin/service awicp_ap_snmp_monitor restart

If the WiDirect gets its IP address using DHCP, the following command may be used to get a new IP address:

sudo /sbin/service network restart

2.5 Restart Watchdog Process

If the Watchdog process fails for any reason it can be restarted from the command line with this command:

sudo /sbin/service awicp_watchdog restart

2.6 Generate SSL Key and Certificate

It is important to generate a new SSL key and certificate when accepting payments using Authorize.net. To generate an SSL key, run this command:

sudo openssl genrsa –out localhost.key 2048

To create a self signed certificate, run this command:

sudo openssl req -new -x509 -nodes -sha1 -days 365 -key localhost.key > localhost.crt

Run the following command to create a certificate signing request (CSR) for a third part to generate a key:

openssl req -new -key localhost.key -out localhost.csr

View the contents of those files with these commands:

cat localhost.key

cat localhost.crt
cat localhost.csr

The entire contents of the key and certificate files, including the lines that start with hyphens, can be put on the certificate page on the WiDirect to update the certificate.

2.7 Using Emacs to Edit Files

Emacs is a command line text editor that can be used to view and edit various files on the WiDirect. The following command can be used to view the system log:

sudo emacs /var/log/messages

Once the editing window is open you can scroll through with the arrow keys on the keyboard. At anytime you can exit by pressing Control-X, followed by Control-C.

2.8 Configure Port Forwarding

Run this command to modify the internal firewall to configure port forwarding rules:

sudo emacs /etc/sysconfig/iptables

Look for the portion of the file containing the existing NAT rules. You may have to scroll down with the arrow and page down keys. The NAT rules should look like this:
**nat*
:OUTPUT ACCEPT [401:23400]
:POSTROUTING ACCEPT [375:21730]
:PREROUTING ACCEPT [144:12599]
-A POSTROUTING -o eth0 -j MASQUERADE

Add the port forwarding rule. To forward traffic on port 8080 to the local IP 10.4.1.2 on port 80, you would use this rule:
-A PREROUTING -p tcp -d x.x.x.x --dport 8080 -j DNAT --to-destination 10.4.1.2:80

Replace x.x.x.x with the eth0 IP for the local WiDirect or WiClient. When finished editing the file, exit Emacs by pressing Control-X, followed by Control-C. Restart the firewall and client by running these commands:

sudo /sbin/service iptables restart
sudo /sbin/service awicp_client restart

Go to the Firewall page in the GUI and add the IP address to the TrustedIPList. If the IP address is not in the trusted list then the device won't be able to communicate with the internet unless it is logged in.

2.9 Using Tcpdump to Monitor Traffic

A utility called tcpdump is available for monitoring network traffic. This utility is useful for diagnosing connection problems, or for monitoring activity on a network interface. This command can monitor traffic for a single user, or for all traffic on an interface. To exit out of tcpdump at anytime press Control-C. Table 2-1 shows some common tcpdump commands.

Monitor all traffic on eth1 for all users	sudo /usr/sbin/tcpdump -ieth1
Monitor traffic on eth1 for IP 10.4.1.20	sudo /usr/sbin/tcpdump -ieth1 host 10.4.1.20
Monitor traffic on eth1 for MAC 00:11:22:33:44:55	sudo /usr/sbin/tcpdump -ieth1 ether host 00:11:22:33:44:55
Monitor DNS requests on eth1	sudo /usr/sbin/tcpdump -ieth1 port 53
Monitor DHCP requests on eth1	sudo /usr/sbin/tcpdump -ieth1 port 67

Table 2-1: Common tcpdump commands

Note: Instead of typing "*sudo /usr/sbin/tcpdump*" on the above commands, run the "*su* -" command first to get root access. Then run the tcpdump utility by typing "*tcpdump*".

2.10 Using Arping to Test a User's Connection

A common method to test a user's connection is to ping their computer. Many computers have pings blocked by default, so this method isn't always helpful. An alternative method is available, called arping, sends an ARP requests which cannot be blocked on the user's computer. ARP requests won't go through a router though, so to use arping the computer must be on the same Ethernet subnet as the WiDirect. To run the arping command the IP address and interface must be specified. This command will ping the IP 10.4.1.20 on the interface eth1:

sudo /usr/sbin/arping 10.4.1.20 -I eth1

The arping command will show the MAC address of the device with the specified IP address. When finished press Control-C to exit.

2.11 Access SQL database

The WiDirect uses a MySQL database to store configuration information. It is not recommended that you make changes to the database, but it can be helpful to access for certain tasks. To access the database, run this command from the SSH session:

mysql -uportal -pannamysql portal

To exit the MySQL client application at any time press Control-C. The following sections will describe how to perform some basic operations on the database.

2.11.1 Reset failed login attempts

The WiDirect administration pages will block an IP address from logging in after three failed login attempts. If you are getting the error saying you need to wait 15 minutes to login then you can reset the failed attempt counter by running the following command in the MySQL client utility:

delete from AdminLoginAttempts;

2.11.2 Recover GUI Administrator Password

The MySQL client utility can be used to recover a lost administrator password. Run this command to view a list of administrator usernames and passwords:

select username,AES_Decrypt(password, "109a134e99.1900.1800-12a") from admin_users;

2.12 More Information

The WiDirect and WiClient models run on the operating system CentOS. Documentation is available on the CentOS web site www.centos.org that gives a detailed overview of all the capabilities of the WiDirect product.

3 Installation

3.1 Support Services

Support Contact Details
Dedicated Phone Support: +1-443-294-0000
Dedicated e-mail support: support@allcitywireless.com
Self-support: www.allcitywireless.com/support

3.2 Example Network Diagram

The following section describes a possible network deployment scenario Figure 3-1 shows the network layout with a WiDirect server and a client. Each of the clients will have several access points, and will have multiple subnets for users. This example will assume one subnet is for public WiFi users and the other subnet for business customers. The network for business customers will be on a VLAN and have different access plans available with different restrictions. Users on the public network will also have an option to enter a code in for faster access. There will be an additional subnet used for administering the access points.
The following IP addressing scheme will be used on both WiDirects:

Internet IP	192.168.200.2/24
DNS	192.168.200.1
Default Route	192.168.200.1

Table 3-1: Internet Connection Information

Public WiFi Users	10.4.1.0/24
Business Users	10.5.1.0/24

Table 3-2 Subnets Used

WiDirect ETH1	10.4.1.1
WiDirect ETH1, VLAN 200	10.5.1.1
WiDirect ETH1, subinterface	10.1.1.254
NAP	10.1.1.10
SAP1	10.1.1.11
SAP2	10.1.1.12
SAP3	10.1.1.13
SAP4	10.1.1.14

Table 3-3 Specific IP addresses

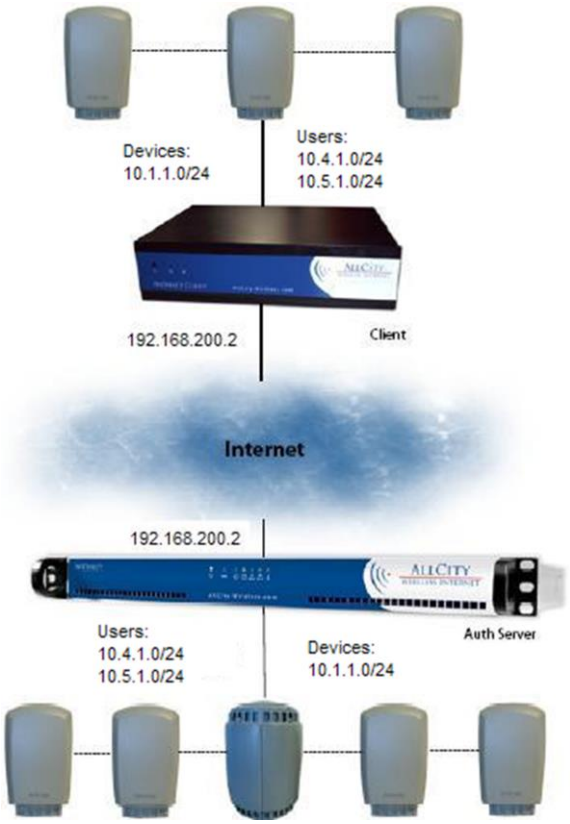


Figure 3-1: Sample Network Diagram

3.2.1 Basic Setup and Configuration

For the most part, the network diagram that is pictured in Figure 3-1 shows a basic WiDirect setup with a client and access points. This addressing scheme is only a suggestion and any IP addressing scheme is valid with the WiDirect.

Before configuring, the first step is to login to the admin page of the WiDirect. See Section 1 on how to access the administration logging page. (By default it is http://10.4.1.1/portal/admin, but can change if the IP addresses have been modified.)

3.2.1.1 WiDirect Network Configurations

The first step in configuring the same network is to configure the Internet information on the WiDirect. It is recommended that the IP address of ETH0 be changed from using DHCP to a static IP address.

NOTE: If you change the IP address of the interface that you are connected to, the connection will drop. You'll need to reconfigure the local IP address of the connecting machine in order to reconnect to the WiDirect. The WiDirect should be restarted when changing the IP address of the ETH1 interface.

In this example, the ETH1 interface is going to remain the same as the default, which is 10.4.1.1/24. However, the ETH0 is going to change to a static IP address with a default gateway as shown in Table 3-1. Figure 3-2 shows the new settings:

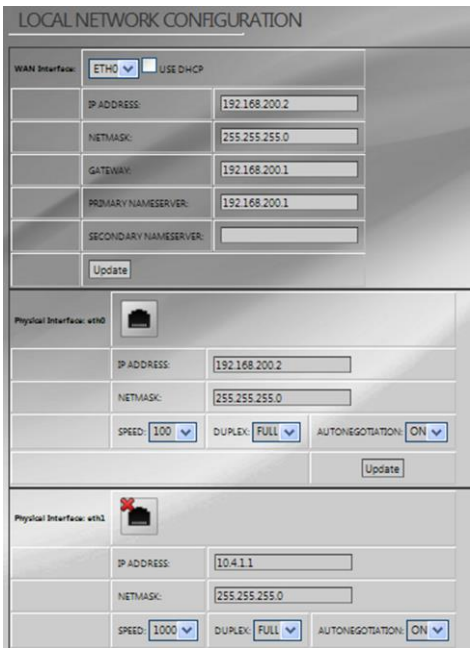


Figure 3-2: Setting up the Network

This example uses a subinterface to communicate with the access points on the 10.1.1.0/24 subnet. Click the **Add Subinterface** button to add the additional IP address on ETH1. The Index ID of 400 is used in the example, but other numbers, such as 1 or 2, would be valid as well.

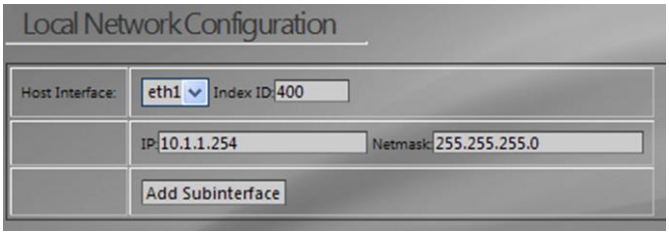


Figure 3-3: Adding Subinterface

This example network will also be using a VLAN. Click the **Add VLAN** button and set the appropriate IP address and subnet mask for VLAN 200.

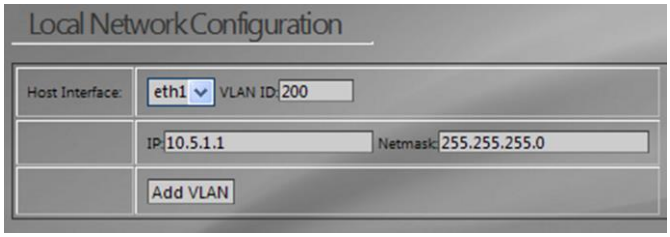


Figure 3-4: Configuring VLAN Interface

3.2.1.2 Configure Firewall

The firewall will have to be modified to listen on the VLAN interface. If the firewall is not configured to listen on the VLAN interface, then that traffic will be allowed to the internet without authentication. Open the **Firewall** page to add the VLAN interface as a gateway interface by adding the line "GatewayInterface eth1.200" in the location described in Figure 3-5.

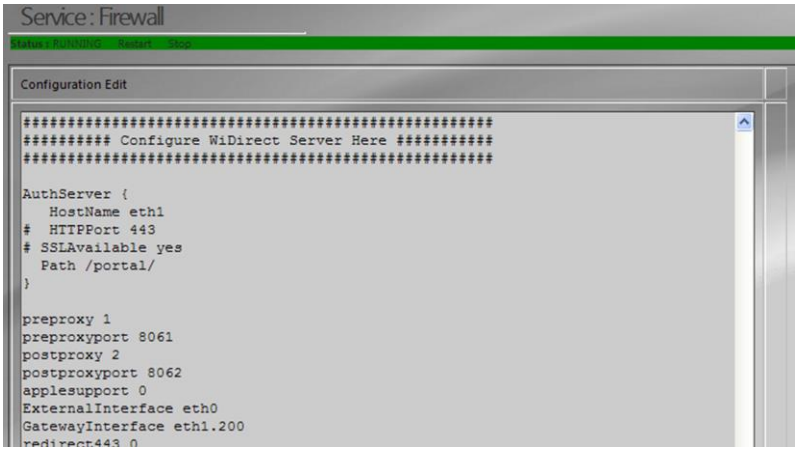


Figure 3-5: Add Gateway Interface

3.2.1.3 Configuring WiClient

The WiDirect Client must be configured with the location of the WiDirect Authorization Server. This setting can be left alone on the WiDirect Authorization Server. This setting can be accessed on the **Firewall** page. Find the part of the file where the hostname of the main WiDirect server is defined. By default it will be "eth1" and it should be changed to the hostname or IP address of the main WiDirect server.

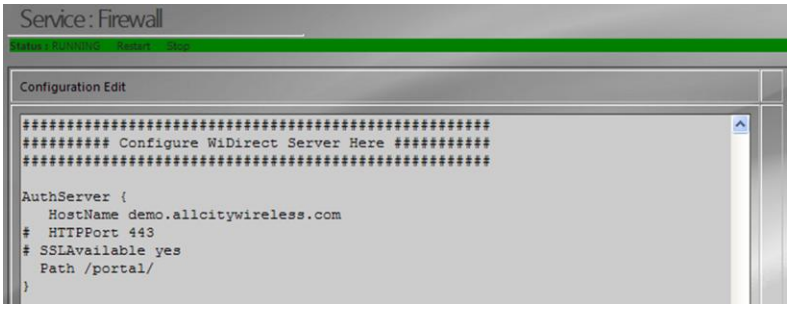


Figure 3-6: Configure WiClient with WiDirect Server Information

3.2.1.4 Configure DNS

Since this example uses a VLAN interface, the WiDirect must be configured to listen to DNS requests on this interface. The DNS server configuration file can be accessed on the **Services->DNS** page. Find the section of the file shown below, and add the line "interface=eth1.200" for the WiDirect to process DNS requests on the VLAN

interface. Note: Newer WiDirects do not require any changes to the DNS configuration as they are configured to listen on all interfaces by default. If the section shown in figure 3-7 is missing then this step may be skipped.

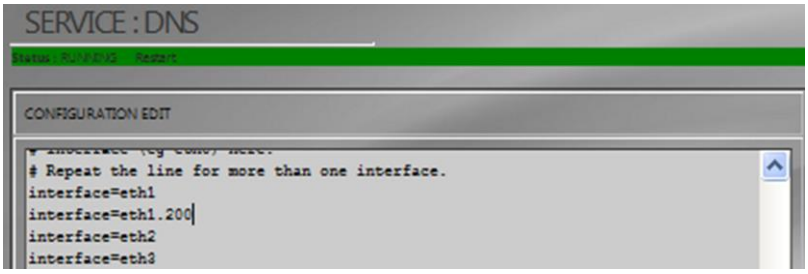


Figure 3-7: Configure DNS Server

3.2.1.5 Adding Access Points

In this example there are eight access points total. Figure 3-8 shows the page for adding access points. The access points connected to the WiDirect Client should be added on that server. The five access points connected to the main WiDirect should be added on that server.

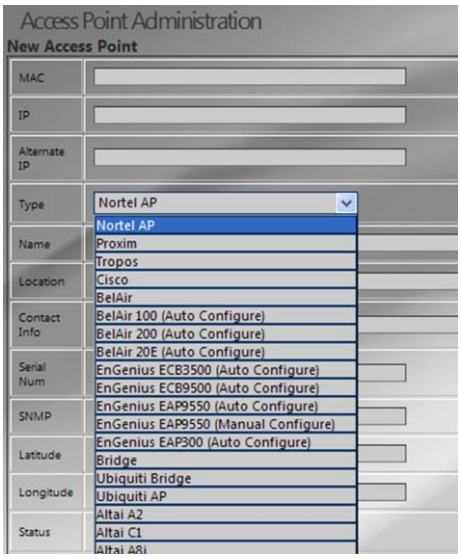


Figure 3-8: Adding Access Point

Figure 3-9 shows the way the access point page should look after all the access points have been added:

MAC	IP	Type	Name	Serial	Location	Contact	Snmp	Mode	Username	Create Date	
00:00:00:00:00:01	10.1.1.10	BELAIR	NAP	BA100		SUPPORT@ALLCITYWIRELESS.COM		ENABLED		WED JUN 1 10:43:34 2011	DELETE
00:00:00:00:00:02	10.1.1.11	BELAIR	SAP1	BA101		SUPPORT@ALLCITYWIRELESS.COM		ENABLED		WED JUN 1 10:43:28 2011	DELETE
00:00:00:00:00:03	10.1.1.12	BELAIR	SAP2	BA103		SUPPORT@ALLCITYWIRELESS.COM		ENABLED		WED JUN 1 10:43:23 2011	DELETE
00:00:00:00:00:04	10.1.1.13	BELAIR	SAP3	BA104		SUPPORT@ALLCITYWIRELESS.COM		ENABLED		WED JUN 1 10:43:17 2011	DELETE
00:00:00:00:00:05	10.1.1.14	BELAIR	SAP4	BA105		SUPPORT@ALLCITYWIRELESS.COM		ENABLED		WED JUN 1 10:44:32 2011	DELETE

Figure 3-9: All Access Points Added

3.2.1.6 Verifying DHCPD configuration

Only minor changes need to be made to the DHCP configuration file for this example. The configuration file can be found on the **Services->DHCP** page. The subnet section in the DHCP server configuration file needs to be modified to include the 10.5.1.0/24 subnet. The subnet section of the file should look like this:

```
# Private Subnet 10.4.1.0/24
subnet 10.4.1.0 netmask 255.255.255.0 {
   range 10.4.1.20 10.4.1.254;
   option routers 10.4.1.1;
   option domain-name-servers 10.4.1.1;
   option ntp-servers 10.4.1.1;
   option subnet-mask 255.255.255.0;
}

subnet 10.5.1.0 netmask 255.255.255.0 {
   range 10.5.1.20 10.5.1.254;
   option routers 10.5.1.1;
   option domain-name-servers 10.5.1.1;
   option ntp-servers 10.5.1.1;
   option subnet-mask 255.255.255.0;
}
```

3.2.1.7 Add Profile

The WiDirect still needs to know about the profile for branding and reporting purposes. By clicking on ***System Configuration->Profiles***, the profile can be added as in Figure 3-10. For this example there are going to be two profiles:

Figure 3-10: Profile Creation

Rules also have to be created in the firewall to determine which users belong in which profile. Clicking on the **Services**->**Firewall** link will allow you to modify the firewall rules. The 10.4.1.0/24 subnet will be on the PublicWiFi profile, and the 10.5.1.0/24 subnet will be on the BusinessUsers profile. A default profile will also be created as an example. Figure 3-11 shows the configuration file with the profile settings applied.

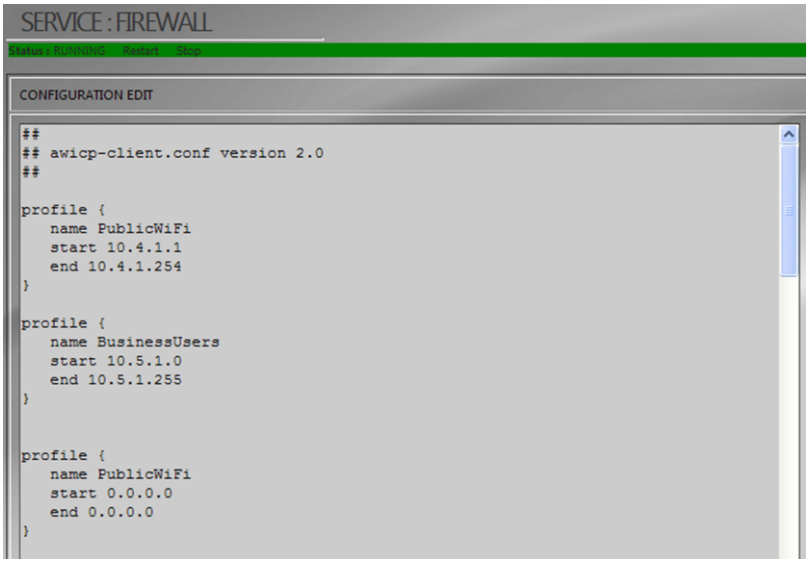


Figure 3-11: Create profiles in Firewall

3.2.1.8 Create Access Plans

For this sample network, two access plans will be created. Figure 3-12 shows the setup for the public plan and Figure 3-13 shows the setup for the business plan. The time restrictions can be left blank for the default values. To prevent the plans from being seen by users on the wrong profile, the profile field should be set properly, and the Default option should be set to No. These settings will make sure that the access plans are only displayed to users on the proper profile.

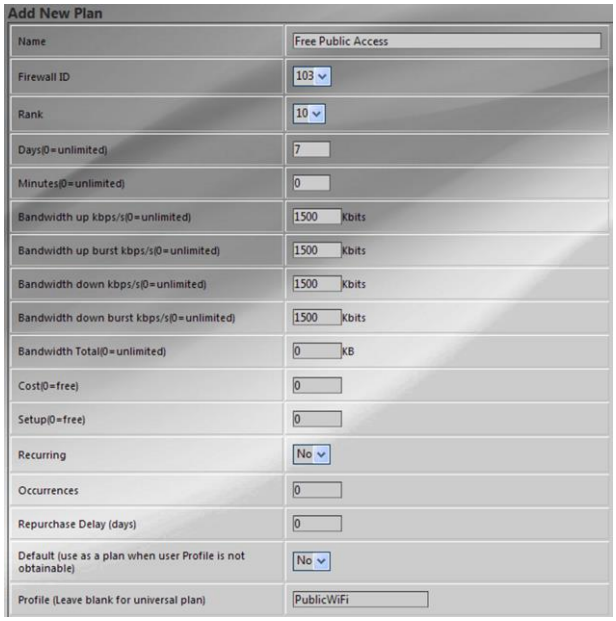


Figure 3-12: Creating the Public Access Plan

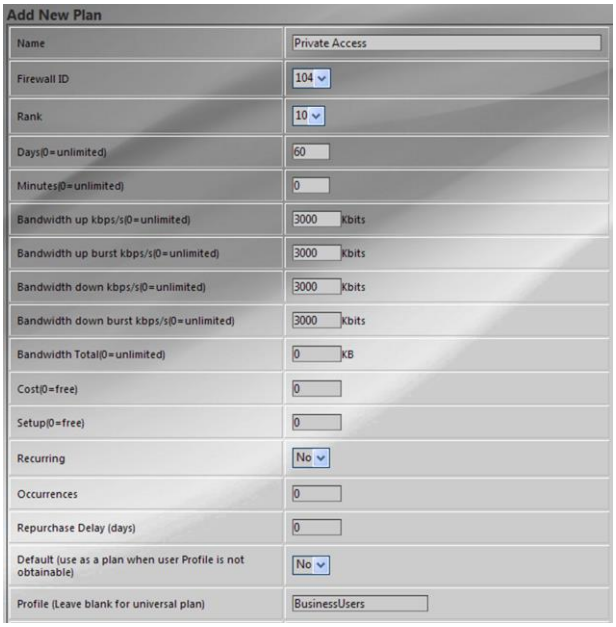


Figure 3-13: Creating the Business Access Plan

3.2.1.9 Create Coupons and Payment Gateway

In this scenario users on the public WiFi network are going to have the option to enter a code for faster access. Any user who knows the code “FastAccess” will be able to enter this code when activating their account to be put on the

faster plan. First create this coupon on the coupon page. The description will be "Public High Speed WiFi Access," the plan will be the public high speed plan previously created, and the token will be "FastAccess." This coupon can be added multiple times so that it can be given to multiple users.

The payment gateway must also be created so that the user is presented with the option to enter a coupon. On the payment gateways screen add a payment gateway with the type coupon, and the profile name "PublicWiFi."

3.2.1.10 Create Administrators

New boxes should have the default administrator password changed and new admin users should be created. See Section 1.6.12.

3.2.1.11 Setting Profile Preferences

Each profile can have its own configuration values. If a different profile setting is required, such as a different redirect page, they can be set in the preferences section. See Section 1.4.1.

3.2.1.12 Branding the User Pages

Setting the branding allows administrators to configure the branding of the user facing pages, such as the login page. If the installation calls for specific graphics and html for these pages, see section 1.4.5.

3.2.1.13 Setting Walled Garden Sites

The walled garden allows access to various sites without login to the WiDirect. These sites vary from depending on the policies of the local network. To configure the walled garden see Section 1.4.2

3.2.1.14 Configuring the Message of the Day

The message of the day allows a message to be displayed on the login page, which is something that needs to be tailored for each installation. This page can be left blank if no message is desired. See section 1.4.4 on how to configure the message of the day.

3.2.1.15 System Check

At this point, all the basic system elements have been configured for this network. Before attempting to login to the Network, click on the **System Check** menu to verify that all the services are enabled and **PASS** the system check. Also, use this page to verify that the IP address is set properly on the ETH0 interface.

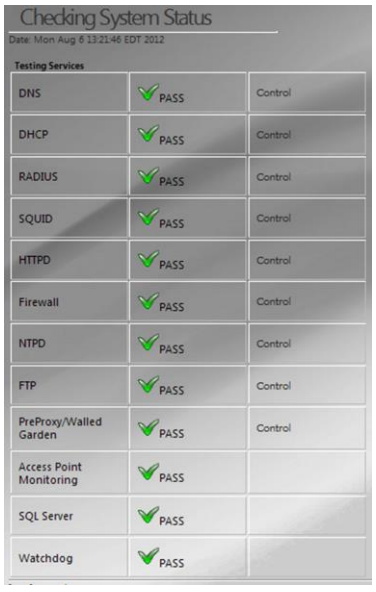


Figure 3-14 Running the System Check

3.2.2 Acceptance Testing of Sample Network

For this network, there are only two features that are required to be tested. The first is the ***AP Status*** page, which verifies that the AP's are up and monitored. The second test is to actually associate to an Access Point wirelessly and test the Internet Connection.

3.2.2.1 *Run AP status to see if the Access Points are up*

Click on the **System Status-> AP Status** link and verify that all the Access Points are UP

3.2.2.2 *Access the Internet Wirelessly*

Using a laptop, physically move to the nearest access point and try to connect to the wireless network**.** If everything has been configured properly, after associating with the access point, the WiDirect will provide the laptop with a DHCP address in the 10.4.1.0/24 subnet.

After an IP address has been provided, open a browser and connect to the Internet. If everything is running properly, the **Captive Portal Login** page will be displayed. Register for an account and login to the network.

At this point, the bare network configuration has been completed. For more system checks, see the **Administration and Maintenance** section later in this document.

4 Special Deployment Scenarios

4.1 Enabling MAC Authentication for Specific Stations

Normally the WiDirect can only run in MAC based authentication mode for all users at once. In other words, MAC based authentication is enabled for all hosts or it is disabled for all hosts.

However, there might be certain situations where only a portion of the devices on your network to be authenticated by MAC address, e.g. hand-held inventory scanners, since they don't have web browsing capability. It is still possible to do this by assigning specific addresses to these devices and then opening the firewall for them. The following steps describe this procedure:

Step 1: Assign a static IP address to each device.

In the DHCPD.conf file (access from the admin page **Services->DHCP**), you can create an entry for each device in the Mobile Node IP pool.
For example, we could assign the IP of 10.8.1.250 to a wireless security camera with a MAC of 00:0F:3D:56:03:43. In the dhcpd.conf file, add the following line.

host camera2 { hardware Ethernet 00:0f:3d:56:03:43; fixed-address 10.8.1.250; }

In this example, the camera is named "camera2," but any name would have been acceptable as long as the name is unique among all the entries in the DHCP configuration file. The MAC address should be entered using all lowercase letters.

Step 2: Add the static IP address to the firewall configuration file.

Access the firewall configuration file from the WiDirect **Admin** page (***Services->Firewall***)

In this configuration file, there is a line called "TrustedIPList", which allows as many IP addresses as needed, as long as they are comma separated. Any IP addresses listed in this line are automatically “passed through" the captive portal without a web based login challenge.

In this example, let's say we had two IP addresses to add 10.8.1.250 and 10.8.1.251.

The configuration file would look like this:

TrustedIPList 10.8.1.250,10.8.1.251

After those two steps have been completed, the devices will be allowed Internet access without being restricted by the captive portal.

4.2 Customizing a Network by Profile

The WiDirect allows you to customize the user's interface and access plan choices based on where they are located in the network. This is done by creating multiple profiles on the network. Users can be placed on a profile based on their IP address or which WiClient they are connected on.

4.2.1 Configure the Profiles

The easiest way to separate the users on multiple profiles is to put them in different IP ranges. With multiple VLANs available users in one VLAN can be placed in one IP address subnet, and users in another VLAN will be in a different subnet. Those subnets can then be placed in different profiles. If there are multiple WiClients in the network then the WiClients can all share a profile, or each WiClient can be on its own profile.
To see the default profile that users are placed on when connecting can be seen in the firewall configuration file. To view the firewall configuration file, click on **Services->Firewall** in the WiDirect or WiClient's menu. The following shows the default configuration for a profile to apply to users who are not assigned a profile anywhere else:

```
profile {
name AnnapolisWireless
start 0.0.0.0
end 0.0.0.0
}
```

You can specify a different range to put people from a different subnet into a different profile:

```
profile {
name Baltimore-Wireless
start 10.8.1.0
end 10.8.1.254
}
```

4.2.2 Branding

To change the branding for the profiles you will need to first click on the **System Configuration->Profiles** menu item to add the profile. After a profile is added you can change the branding by clicking on the **Profile Branding** menu option.

4.2.3 Access Plans

Users can be given a different choice of access plan based on which profile they are in. When creating an access plan, specify the profile in the profile field to show that access plan to users registering on that profile. Also the default option must be set to no if the plan should not be displayed to all users. If the default option on the plan page is enabled, then the plan will be shows to users on all profiles. The access plan may also be marked as restricted which allows them to only sign in on that profile.

4.3 Configuring VLANs

Configuring VLANs requires changes in a number of different places. First the VLANs need to be created on the network configuration page. Then the DHCP and DNS server must be properly configured to handle those VLANs. Finally the firewall must be configured to require that traffic to be authenticated.

4.3.1 Create VLAN

The bottom of the Network Configuration page has buttons to add a VLAN interface. The pages to add a VLAN or Subinterface are shown in Figures 1-28 and 1-29. To add a VLAN or subinterface you must enter an IP address, netmask, and an ID number from 1 to 4095.

4.3.2 Configure DNS and DHCP Servers

The DNS and DHCP servers both should be configured to handle the VLAN interface. The DNS server will ignore DNS requests unless the interface has been specified in the configuration file. The DHCP server needs to be properly configured to give out IP addresses for the VLAN subnet.

4.3.3 Configure Firewall

By default the firewall will only redirect traffic to the captive portal on the eth1 interface. To force users on the VLAN interface to authenticate with the WiDirect the firewall needs to be told to listen on the VLAN interface.

4.4 Setup Recurring Billing with Authorize.net CIM

This section explains how to configure a WiDirect to automatically charge a user's credit card when their account is due to renew. Configuring recurring billing requires careful configuration of the payment gateways so that the payments are processed properly.

4.4.1 Payment Gateways

You need to add both an Authorize.net payment gateway, and an Authorize.net CIM payment gateway. The regular Authorize.net payment gateway should have the URL "https://secure.authorize.net/gateway/transact.dll" and the status should be set to disabled. The status is disabled because it won't show up on the payment option list by default, but it still may be used internally if a user signs up for a non-recurring plan and chooses not to save their credit card information. The login and key should be set to the API login and key provided by Authorize.net.
The Authorize.net CIM payment gateway should be added on the payment gateway page with the URL "https://api.authorize.net/xml/v1/request.api" and the status should be active. There should be no other Authorize.net payment gateways created.

4.4.2 Access Plans

To make an access plan bill automatically set the "Recurring" option to "Yes" and set the number of occurrences to be the number of times that the plan will bill. Use a large number for the occurrences to make it bill indefinitely.

4.4.3 User Details

Users who have an active Authorize.net profile will have that information listed on their user details page. That profile must be removed before the user can be deleted.

4.4.4 Email Templates

There are branding options for the successful and failed payment e-mails. These are currently only pulled from the "default" profile, so you will need to add a profile called "default" to edit them. The payment e-mails will come from the address specified on "Email Support Address" option on the preferences page,. The payment emails will also CC to that address. Emails are only sent for automatic payments, not initial payments.
You can also edit the branding of the account edit page. The account edit page is where a user can update their account or credit card information. You will want to link to this page from the failed payment e-mail so they can update their information if their card is declined.

4.4.5 Failed Payments

If a user has an active profile with Authorize.net and their card is declined the failed payment e-mail will be sent. The user will have an opportunity to update their account information. There will be additional attempts made 24 and 48 hours later. If the payment is still denied on the 3rd attempt then the account will be expired.

4.4.6 Activating Accounts

If there is an old expired account that still has a payment profile with Authorize.net, simply changing the status to be "Active" will bill the user again. Changing a user's status to Active does not change their registration date. A user on a regular plan would be automatically expired again. A user on a recurring plan will be billed again.
The proper way to reactivate a user with a new registration date is to use the **Change User Plan** option at the bottom of the user details page. This will mark the account active, and will prevent an immediate attempt to expire/charge the account again.

4.4.7 Making a Payment

When signing up for a recurring plan the user is of course forced to save their credit card information. If they are making a one-time payment they have the option of either saving their credit card information or not saving it. If the

user does choose to save their credit card information then the next time they renew they have the option of using their old credit card.

4.4.8 Update Account

Users can edit their credit card information by going to https://www.widirectdomain.com/update. It would be helpful to give links to this page from the login page and failed payment e-mails so users know how to update their credit card information. This is only used for accounts that are active on a recurring plan.

4.5 Turning off External DNS Resolution

In some deployments, if DNS service is unstable, disabling it at the WiDirect allows the mesh to remain up during DNS server outages. Only the DNS service at the mobile nodes will be interrupted instead of the entire mesh.

To perform this operation, command line access is required on the WiDirect. Login via ssh to the WiDirect.

Step 1: Edit the /etc/nsswitch conf file

Run the command *sudo vi /etc/nsswitch.conf*. Look for the line that reads "host : files dns" and change it to say "hosts: files"

Step 2: Edit the /etc/resolv.conf file

Run the command *sudo vi /etc/resolv.conf* file. Any lines that say "nameserver" add a "#" to the beginning of the line.

Step 3: Edit the ap.ftp file

Use the gui **Admin** page and click on ***Nortel Support->Ftp***. Look for entries in the dhcpd file that being with "domain-name-server", there should be at least two entries, all of them need to be changed to the IP address of the upstream DNS server. This is the same IP address that was added in the network configuration window of the WiDirect.

Step 4: Reboot the mesh

At this point, the entire mesh will need to be restarted for the DNS changes to take effect.

4.6 Hiding Access Plans from Users

Hidden access plans can be created that are not displayed to users. If a profile is set on an access plan to an unused profile, and the default option is set to no, then the access plan won't be displayed to users. Another way to hide an access plan is to choose "hidden" in the rank menu.

Figure 4-1: Creating a hidden access plan

4.7 Entering Ingress (From Internet) Firewall Rules

The WiDirect software uses iptables to manage the firewall. When the WiDirect starts up, it uses iptables to define new firewall rules. However, the default firewall rules can be modified by the Administrator. The default iptables file that is shipped with the WiDirect looks like this:

```
*filter
:FORWARD ACCEPT [0:0]
:INPUT DROP [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -i eth0 -p tcp -m tcp --dport 22 --tcp-flags SYN,RST,ACK SYN -j ACCEPT
-A INPUT -i eth0 -p tcp -m tcp --dport 80 --tcp-flags SYN,RST,ACK SYN -j ACCEPT
-A INPUT -i eth0 -p tcp -m tcp --dport 443 --tcp-flags SYN,RST,ACK SYN -j ACCEPT
-A INPUT -i eth0 -j REJECT --reject-with icmp-port-unreachable
-A INPUT -p tcp -m tcp --dport 8060 --tcp-flags SYN,RST,ACK SYN -j ACCEPT
-A INPUT -p tcp -m tcp --dport 8061 --tcp-flags SYN,RST,ACK SYN -j ACCEPT
-A INPUT -p tcp -m tcp --dport 8062 --tcp-flags SYN,RST,ACK SYN -j ACCEPT
-A INPUT -p tcp -m tcp --dport 20 --tcp-flags SYN,RST,ACK SYN -j ACCEPT
-A INPUT -p tcp -m tcp --dport 21 --tcp-flags SYN,RST,ACK SYN -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 --tcp-flags SYN,RST,ACK SYN -j ACCEPT
-A INPUT -p udp -m udp --dport 53 -j ACCEPT
-A INPUT -p udp -m udp --dport 67 -j ACCEPT
-A INPUT -p udp -m udp --dport 68 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 7911 -j ACCEPT
-A INPUT -p udp -m udp --dport 123 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 123 -j ACCEPT
-A INPUT -p udp -m udp --dport 514 -j ACCEPT
-A INPUT -p icmp --icmp-type 0 -j ACCEPT
-A INPUT -i eth1 -p icmp --icmp-type 8 -s 0/0 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p tcp -m tcp --dport 443 --tcp-flags SYN,RST,ACK SYN -j ACCEPT
-A INPUT -p tcp -m tcp --dport 1813 --tcp-flags SYN,RST,ACK SYN -j ACCEPT
-A INPUT -p udp -m udp --dport 1813 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 1812 --tcp-flags SYN,RST,ACK SYN -j ACCEPT
-A INPUT -p udp -m udp --dport 1812 -j ACCEPT
-A INPUT -i lo -j ACCEPT
COMMIT
# Completed on Sun Jun  4 17:19:16 2006
# Generated by iptables-save v1.3.0 on Sun Jun  4 17:19:16 2006
*nat
:OUTPUT ACCEPT [401:23400]
:POSTROUTING ACCEPT [375:21730]
:PREROUTING ACCEPT [144:12599]
-A POSTROUTING -o eth0 -j MASQUERADE
COMMIT
```

These rules can be modified as Administrators see fit. (See the Disabling NAT section 4.9 in this document for an example.) To edit this file, connect to the command line interface and run the following command:

sudo vi /etc/sysconfig/iptables

After editing the file, it is best to reboot the WiDirect for the changes to take effect due to the amount of software that relies on the iptables file.

For more information on editing the iptables file, consult the netfilter documentation at:
http://www.netfilter.org.

4.8 Disabling DHCP Dependency

An often overlooked aspect of the DHCPD configuration file is to disable DHCP service on the ETH0 (Internet facing) interface. In order to do this, add an entry to the dhcpd configuration file that instructs dhcpd to ignore Eth0's IP range.

For example, if Eth0's IP and subnet was 192.168.20.2 with a subnet mask of 255.255.255.0. A "blank" configuration line for this subnet would be needed in the dhcpd configuration file to tell DHCP not to provide service on this interface. The dhcpd.conf line looks like this

subnet 192.168.20.0 netmask 255.255.255.0 {}

When DHCPD starts up, it sees this as not needing to provide dhcpd to this IP space and will 'disable' DHCP on the ETH0 interface.

4.9 Disabling NAT **(Network Address Translation)**

If you want to provide routable IP space to your Mobile Nodes, you can disable NAT on your WiDirect. In order to do this, you must be familiar with a command line editor such as VI or EMACS. In this example, we'll show the VI commands.

If you are disabling NAT, you will need a routable subnet on intranet and extranet networks. You can still use private subnets such as 10.0.0.0/8, as long as it's routable beyond the WiDirect box. The WiDirect is just going to act as a firewall without NAT enabled.

SSH to the WiDirect and run the following command:

sudo vi /etc/sysconfig/iptables

Use the arrow keys to find this line:

-A POSTROUTING -o eth0 -j MASQUERADE

Comment out this line by adding a "#" in front of it. Save the file and exit the VI editor.

After making those changes run these two commands for the changes to take effect:
sudo /sbin/service iptables restart
sudo /sbin/service awicp_client restart

4.10 Enable Ping on WAN Interface

By default the WiDirect does not respond to pings on the WAN interface. To enable pings you need to modify the iptables configuration file on the WiDirect.

SSH to the WiDirect and run the following command:

sudo vi /etc/sysconfig/iptables

Use the arrow keys to find this line:

-A INPUT -i eth0 -j REJECT --reject-with icmp-port-unreachable

Above that line add a new line that looks like this:

-A INPUT -i eth0 -p icmp --icmp-type 8 -s 0/0 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

Save the changes and exit the vi text editor. Then run these two commands for the changes to take effect:

sudo /sbin/service iptables restart
sudo /sbin/service awicp_client restart

4.11 How to Disable Mobile Node Access to the Admin Pages

On some networks, more security might be required for the WiDirect Admin pages. In fact, it's recommended that this security measure be added anywhere there isn't tight security on the network.

The WiDirect admin page has built in security where five failed login attempts will lock out an IP address for 15 minutes. However, if needed, it is possible to disable admin login page attempts completely from the Mobile Network. In order to do this, SSH to the WiDirect and run this command.

sudo vi /root/AWICP/www/portal/admin/.htaccess

In this file add the following lines.

*<Files *>*
order allow,deny
allow from all
deny from 10.8.1.0/24
</Files>

Change the 10.8.1.0/24 to be the IP subnet range of your mobile network. Run this command next:

sudo vi /etc/httpd/conf/httpd.conf

Look for the section of the file that looks similar to this:

<Directory "/var/www/html">
Options Indexes FollowSymLinks
AllowOverride AuthConfig Limit
Order allow,deny
Allow from all
</Directory>

Change the line that reads “AllowOverride None” to be “AllowOverride AuthConfig Limit”. After making that change, exit the file and restart the Apache service by running this command:

sudo /sbin/service httpd restart

4.12 Login and Logout URL

On some networks, it might be desirable to allow users to completely logoff of the WiDirect instead of letting them timeout. This can be accomplished by providing a ***Logout*** button to the users on an external web page on a different server. If there is a homepage that users have access to, the following URL can be used on that page to create a ***Logout*** button.

http://10.4.1.1:8060/awicp/logout

There may also be instances where you want to give users a link to login, such as when you redirect users to a landing page instead of the login page. The login page can be accessed at the following URL:

http://10.4.1.1:8060/

In both instances, change the 10.4.1.1 IP address to the IP address of Eth1 interface of the WiDirect.

Note: Only the Eth1 IP address can be used.

4.13 Sendmail SMTP Configurations

Depending on the deployment, most networks have a special SMTP Relay through which email must be sent in order to leave the network. In other words, the WiDirect will not be able to send output email without relaying through the SMTP relay host.

The email/SMTP controller that runs on the WiDirect is called Sendmail, which is a standard SMTP process that runs on most servers. In order to configure Sendmail, an Administrator must SSH to the WiDirect and edit the Sendmail configuration with the following command:

sudo vi /etc/mail/sendmail.cf

4.13.1 Updating the SMTP domain name

In this file, there are several fields that can be modified. The first setting is the "domain name" of the WiDirect, which is used to explicitly tell Sendmail what domain to use when addressing outbound email. For example, if the local network's domain was "companyxyz.com", find the following lines in the sendmail.cf file:

```
# my official domain name
# ... define this only if sendmail cannot automatically determine your domain
#Dj$w.Foo.COM
```

And change it to:

```
# my official domain name
# ... define this only if sendmail cannot automatically determine your domain
Dj$w.companyxyz.com
```

4.13.2 Adding an SMTP Relay

If a SMTP email is required on the network, this can be done by adding a DS entry to the sendmail.cf file. Find the line in the sendmail.cf that looks like this:

```
# "Smart" relay host (may be null)
DS
```

If the local SMTP relay was smtp.companyxyz.com, change these lines to read:

```
# "Smart" relay host (may be null)
DSsmtp.companyxyz.com
```

4.13.3 Restarting the Sendmail Process

After making changes to the sendmail.cf, Sendmail can be restarted via an init script or simply rebooting the WiDirect. To restart the process from the CLI, use the following command:

/etc/init.d/sendmail restart

4.14 Hosted WiDirect

The Hosted WiDirect service is available to allow network operators to quickly deploy a wireless network without purchasing a WiDirect. A WiClient is placed at each location and told to point back to the data center hosted by AllCity Wireless.
The GUI on the Hosted WiDirect is very similar to a regular WiDirect, but several features are removed from the interface as they are not required. The **Services** menu is removed since all the services run on the WiClient. Likewise the pages to add and configure access points are not on the Hosted WiDirect.

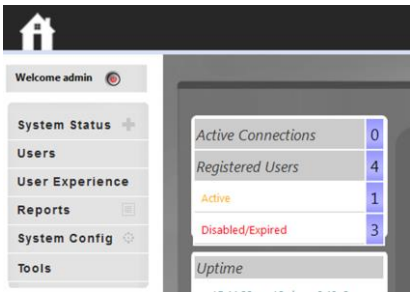


Figure 4-2: Hosted WiDirect Menu

4.15 Disable Proceed Page When Using MAC Authentication

When MAC based authentication is used, the users will be brought to a splash page asking them to hit a button before connecting to the network. The purpose of this page is to give the user a consistent experience, and to avoid the problems when the user tries to login too many times simultaneously.
If you plan to disable the proceed page then the first thing you need to do is to open the **Access Plan** page and increase the number of concurrent logins allowed for each access plan. The default value is one, and you will want to increase that to a higher number, such as 15.
The next step is to modify the login page to automatically bypass this screen. From an SSH session, run the following command:

sudo emacs /root/AWICP/etc/config.php

Scroll down to find this line:

$displayLoginMacAuth = 1;

On that line change the 1 to a 0, and exit by pressing Control-X followed by Control-C. After making the above changes users will no longer see the proceed page. The users will still have to open a web browser before accessing the internet.

4.16 Automatically Logout Dead Connections

Sometimes a user's connection data counters will report no traffic even though the user has been on for a while. While these connections are not a problem, it makes the active users page look better to have these extra connections removed. There is a setting to log these connections out quicker than the idle timer if that is desired. Run this command from the command line:

sudo emacs /root/AWICP/bin/awicp_manager.pl

Look for a line that says "my $MAX_DEAD_SECONDS = 0;" Change the 0 to the number of seconds a connection with 0 data should be allowed to stay open.

4.17 Increased Customization of Login Page

The WiDirect includes some of the login page branding directly in the login page PHP files by default to make branding easier. To get full control over the look and feel of the login page, this extra branding code can be removed. To remove this extra code open the login page PHP file with this command:

sudo emacs /root/AWICP/etc/config.php

Scroll down to find this line:

$showLoginText = 1;

On that line change the 1 to a 0, and then exit the emacs text editor. The next step will be to modify the login template. The following code will display the default login template when the regular login branding is disabled:

```
<html>
<head>
<link rel="stylesheet" href="/portal/branding//default//style.css" type="text/css">
</head>
<body background="/portal/branding//default//images/bg_body.jpg">
<br>
<br>
<div id="ctr" align="center">  <div class="login">    <div class="login-form">      <img
src="/portal/images/login.gif" alt="Login">
<div class="form-block">
%%LOGIN_FORM%%
</div>
</div>
<div class="login-text">
<p>Welcome to Network Network</p>
<p>Please enter a valid username and password to access the system.</p>
<br><h3>Need an account?</h3>
<a href="/portal/register/?ssid=%%PROFILE%%&mac=%%MAC%%&ap=%%AP%%&url=%%URL%%">Click
here to register</a></h3>
</p></div>
<div
class="clr"></div><p><A  href="/portal/forgot/?ssid=%%PROFILE%%&mac=%%MAC%%&ap=%%AP%%&url
=%%URL%%">Forgot
Password?</A></p><p><A  href="/portal/changepassword/?ssid=%%PROFILE%%&mac=%%MAC%%&ap=%%
AP%%">Change Password</A></p>      </div>
</div>
</div>
</body>
</html>
```

4.18 Enable SNMP Monitoring of the WiDirect

SNMP monitoring is available on the WiDirect to help the administrator monitor functions of the device. The following commands will install and enable the SNMP server.

yum install net-snmp.i386
service snmpd start
chkconfig snmp on

That will give you basic SNMP information. The SNMP port must be opened on the WiDirect as well. Run this command to edit the firewall:

emacs /etc/sysconfig/iptables

To open the SNMP port add this line:

-A INPUT -p udp -m udp --dport 161 -j ACCEPT

That line must be added before this line:

-A INPUT -i eth0 -j REJECT --reject-with icmp-port-unreachable

Save and exit the file. Restart the necessary processes with these commands:

service iptables restart
service awicp_client restart

The SNMP configuration may be edited by changing the /etc/snmp/snmpd.conf file. When making changes to the SNMP configuration file restart the SNMP service with this command:

service snmpd restart

4.19 Automatic Login on Multiple Devices

Normally MAC based authentication only works for the last device to login on an account. If the user logs in with a second computer, then only the second computer will automatically login the next time. An exception is for access plans that have a device limit. If an access plan has a device limit, then the extra MAC address list will be automatically populated as the user connects with more devices. An administrator can also manually add a MAC address to a user's account on the user details page. There is a section at the user details page to add an extra MAC address to an account for automatic login.
The WiDirect can also be customized to automatically add MAC addresses to an account when a user connects. Run this command on the WiDirect to change that setting:

sudo emacs /root/AWICP/etc/config.php

Look for a line that says "$autoAddMac = 0;" and change it to read "$autoAddMac = 1;". The WiDirect can be configured to automatically delete extra MAC addresses when an account expires. To have the WiDirect automatically delete the MAC addresses of expiring accounts first run this command:

sudo emacs /root/AWICP/bin/awicp_manager.pl

In that file look for a line that contains "$deleteExtraMacsOnExpire = 0" and change the 0 to a 1. Then run this command to restart the service:

sudo /sbin/service awicp_manager restart

To automatically delete the MAC addresses when an administrator expires an account, run this command:

sudo emacs /root/AWICP/etc/config.php

In that file look for the same "$deleteExtraMacsOnExpire = 0" part and change the 0 to a 1.

4.20 Throttle Bandwidth after Limit Reached

When a bandwidth cap is set on the access plan page a user's account will be marked as expired when the cap is reached. Another option is available, which will reduce the user's available bandwidth setting for the remainder of their current plan period. To enable this setting first run this command to edit the config.php file:

sudo emacs /root/AWICP/etc/config.php

In that file change the line that says "$showThrottleSpeed = 0" to "$showThrottleSpeed = 1" to enable the throttled speed options to be displayed on the access plan page. After making the change there will be additional options on the plan page to handle how accounts are handled after the bandwidth quota is reached. Turn the throttle option to on, and set the desired bandwidth for the users after the quota is reached. Figure 4-3 shows the settings to restrict users to 1 Mb/s after they have transferred a gigabyte of data.

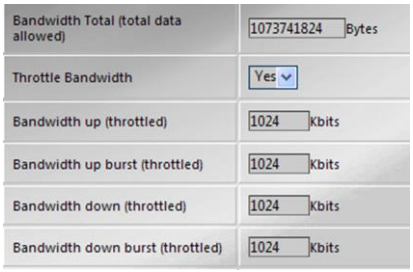


Figure 4-3: Throttled Bandwidth Option

4.21 Configure SmartEdge Authentication

4.21.1 Modify configuration files

To configure SmartEdge authentication a number of command line settings must be configured. After connecting to the WiDirect over SSH type the command "sudo nano /etc/raddb/modules/smartedge" and the contents of that file should be updated to look like this:

```
smartedge {
        forwardpolicy = "in: captiveportal"
        widirectserver = "127.0.0.1"
        sharedsecret   = "widirect"
}
```

Be sure to update the forward policy and shared secret to the appropriate values.
Run "sudo nano /etc/raddb/sites-available/default" and add the text "smartedge" to both the "authorize" and "accounting "sections. The "smartedge" line in about the middle of the appropriate section.

4.21.2 Modify GUI Settings

Be sure the client name and shared secret is added to the clients.conf file as well. This file can be modified directly through the GUI page on the WiDirect. The Radius page is under the Services menu.
On the WiDirect there is a SmartEdge menu item under the System Config menu. On the SmartEdge page you can enable SmartEdge support for a profile, and set a number of paramaters. Included on that page are the forward policy, shared secret, WiDirect IP, and SmartEdge IP. Some of these settings may duplicate the settings above, but must be properly set in all places.

4.22 Configure UAM

The WiDirect will allow for authentication with devices that support the UAM protocol. To allow for this authentication the subnet the access points are on must be added in the Radius client with an appropriate subnet and a UAM secret must be set on the UAM page.

A number of command line changes are required to make UAM authentication work. The API must be enabled by modifying the "/root/AWICP/etc/api-config.php" file. Be sure the value "true" is set on the api_enabled line. Also set a desired username and password. Next run "nano /etc/raddb/modules/widirectuam" and update the file to look like this:

```
widirectuam {
  widirectserver = "127.0.0.1"
  widirectusername = "user"
  widirectpassword = "pass"
}
```

When modifying the above file be sure to enter the appropriate API username and password. The access point should be configured to point to /portal/uam/ in addition to being configured with the proper RADIUS and UAM secrets. Figure 4-4 shows an Ericsson access point configured to use UAM.

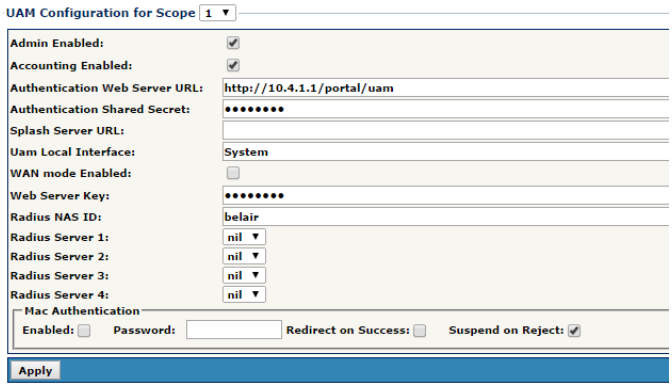


Figure 4-4 Ericsson Access Point UAM Config.

4.23 Performing a System Backup

In order to backup the WiDirect, SSH to the WiDirect (Section 2.1) and run the following commands:

cd /root/AWICP/bin
sudo ./doBackup.sh

This will create a backup image of the WiDirect. After the backup is complete, the system will prompt:

Would you like to burn this backup directly to a CD[y/n]

If a CD backup is desired you must connect a USB recordable CD drive to the WiDirect, insert a BLANK recordable CD into a USB CD drive and enter 'y'. Otherwise, type 'n' and Enter.

After the backup is complete, the WiDirect will tell you where the backup tar file is on the WiDirect, which can be retrieved via SCP to another server.

Dump complete. You can pull the file from /root/backup-XXXXXX.tar.gz

To SCP the backup file to another server, use this command:

scp /root/backup=XXXXXX.tar.gz username@a.b.c.d:.

(Where username and a.b.c.d are actual hostanames and IP addresses)

Backup files can also be saved to a thumb drive with the following commands:

sudo mount /dev/sdb1 /mnt
sudo cp /root/backup-XXXXXXXX.tar.gz /mnt/.
sudo umount /dev/sdb1

4.24 Performing a System Recovery

In order to restore a backup, SSH to the WiDirect (Section 2.1) and copy the backup file to the WiDirect into the /tmp directory. This can be done several different ways as described below.

SCP

s*udo scp username@a.b.c.d:backup-XXXXX.tar.gz /tmp/.*

CD-R

sudo mount /dev/cdrom /mnt
sudo cp /mnt/backup-XXXXXX.tar.gz /tmp/.
sudo umount /dev/cdrom

Thumbdrive

sudo mount /dev/sdb1 /mnt
sudo cp /mnt/backup-XXXXXX.tar.gz /tmp/.
sudo umount /dev/sdb1

Once the backup file is run on the WiDirect, perform the backup with the following commands.

1. CD to the tmp directory

cd /tmp

2. Gunzip the file

sudo gunzip /tmp/backup-XXXXXX.tar.gz

3. Untar the file. Use this tar command with the exact options

sudo tar xfP /tmp/backup-XXXXXX.tar

4. Cd to the newly created directory, which will always be /root/backup-XXXXX

cd /root/backup-XXXXXX

5. Run the backup command

NOTE: Run this command from this directory only (as described in step 4)

sudo ./recoverBackup.sh

6. Reboot the WiDirect

sudo reboot

Note: If you are performing a recovery to a new physical WiDirect, a new license will need to be installed after the recovery. Contact support@allcitywireless.com for a new license.

4.25 Modify Custom Configuration Settings

The WiDirect and WiClient contain numerous custom configuration variables in two files. Tables 3-1 and 3-2 describe the most commonly used settings in the two files. The two files can be modified with these commands:

sudo emacs /root/AWICP/etc/config.php
sudo emacs /root/AWICP/etc/config.pl

Variable	Default	Description
$logLoginFailures	0	Set to 1 to log all failed login attempts. A report is available on the reports page.
$defaultUsername	array()	Use to specify a default username for a profile. Each profile can have a separate default username. For example: $defaultUsername = array(); $defaultUsername[“profile1”] = “profile1user”; $defaultUsername[“profile2”] = “profile2user”;
$verifyComputerAlso	true	For free trial plans this determines whether the MAC address is also verified as having used the plan before. Set to false to only restrict based on whether the account has used the plan before.
$verifyPlanForCoupon	false	Set to true to force free trial restrictions on a user using a coupon. By default a user with a coupon code can activate an account, even if the plan normally wouldn’t be available to a user because they had selected the plan too recently.
$useCouponDiscounts	false	Set to true to allow coupons to be used to discount the price of the access plans. If this option is enabled then entering a coupon code will display a new list of plans having a profile name matching the code entered.
$registrationDateEditable	false	Set to true to allow the registration date to be editable from the user details page.
$showSimultaneousConnections	0	Set to 1 to add an option to modify the number of simultaneous connections a user is allowed. This setting will override the user’s plan setting.
$deleteExtraMacsOnExpire	0	Set to 1 to clear out a user’s extra MAC table when an account is expired by an administrator. This option is useful if an account as a device limit.
$usernameEditable	0	Set to 1 to allow the username field to be edited on the user details page.
$showMoreReports	0	Enable to view some custom reports
$enableRefund	0	Set to 1 to enable refunds for Authorize.net CIM payments.
$showInvalidPassword	0	Set to 1 to show the invalid password entered by the user in the log files.
$showThrottleSpeed	0	Set to 1 to enable the access plan options to set a reduced speed for a user after a bandwidth cap is used.

Table 2-2: Common config.php configuration options

$storeTrackingData	0	Set to 1 to enable logging of user signal strength history for supported access points.
$MAX_DEAD_SECONDS	0	This value allows a separate idle timeout for users that pass no traffic. The default value will just keep the user on for the regular idle time.
$deleteExtraMacsOnExpire	0	Set to 1 to clear out a user’s extra MAC table when an account expires. This option is useful if an account as a device limit.

$logActiveUsers	0	Set to 1 to keep a running count of the number of active users each day. This information is viewable on the reports page.

Table 2-3: Common config.pl configuration options

5 Administration & Maintenance

5.1 Active Users

A list of active users can be displayed. It will provide the locale they are in while accessing, how long they have been on, and how much traffic they have passed. A button is available to log the user off. Other information available is the current IP address and MAC address of the user.

5.2 Event Viewer

Under the Event Viewer various messages are displayed with the severity of the event and a timestamp. If Access Points are rebooting or Clients are unresponsive the event viewer will report it, as well as the last time an Administrator logged into the WiDirect Management Console. The ***Event Viewer*** is also able to be sorted by date, severity, or event description.

5.3 AP Status and Transit Link Graph

The Transit Link (TL) Graph is a visual representation of Access Points communicating with each other. The TL graph will show if all APs are connected and the strength of the TL signal between them. If an AP is orphaned, it will not show a connection to the other access points.

5.4 System Check

By clicking on ***System Check,*** the WiDirect displays a list of all the services the WiDirect is running. Green checks indicate that all systems are functioning properly. If a service is not running it can be forced to restart. Below the services information portion of the page is information that pertains to connectivity. IP, Time, and routing information are available on the ***System Status*** page.

5.5 System Verification

5.5.1 Verify Processes

Under the **Admin** page, there is a ***System Status->System Check*** button. This page analyzes all the running processes and provides an up/down status for each. If for any reason a process is disabled, you can click on the ***Control*** button next to each process in order to re-enable it.

As for the WiDirect specific processes, there is an internal watchdog program that will automatically restart any WiDirect process that should be running.

5.5.2 Verify Captive Portal Features

Once the WiDirect has been setup, verification of the Captive Portal features requires a laptop to be able to associate to the Wireless mesh. Once connected to an Access Point, try connecting to a web page such as www.google.com. If

the Captive Portal is working properly (and www.google.com is not in the walled garden), the WiDirect will intercept the web request and present the Captive Portal Login page.

5.5.3 Speed Testing

The WiDirect has built in speed monitoring software. To view the output of this program in real time, SSH into the WiDirect box as user '**portal**' and execute this command:

bwm-ng

Another test is to use http://www.speedtest.net while connected to the mesh. This URL allows you to choose a server that is geographically located close to the network. Click on the server to use and a test will automatically run that provides both download and upload speeds.

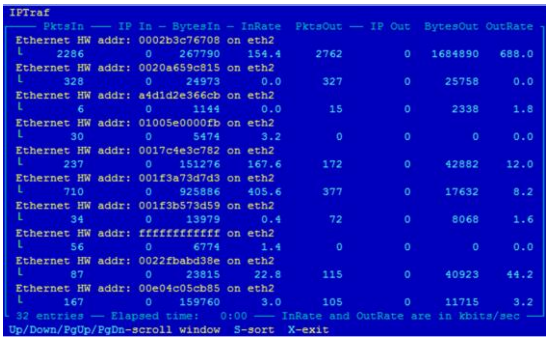
A utility called iptraf is also available to monitor how much traffic is coming from each user on the WiDirect. Run the following command from the command line to install the iptraf utility:

sudo yum –y install iptraf

After the iptraf utility is installed it can be run using the following command:

sudo iptraf

To view the devices currently connected on the wireless network choose **LAN Station Monitor** from the first menu, then choose the interface eth1. The next screen, as shown in figure 5-1, will show the devices currently connected along with how much bandwidth each one is using.


IPTraf
PktsIn IP In BytesIn InRate PktsOut IP Out BytesOut OutRate
Ethernet HW addr: 0002b3c76708 on eth2
2286 0 267790 154.4 2762 0 1684890 688.0
Ethernet HW addr: 0020a659c815 on eth2
328 0 24973 0.0 327 0 25758 0.0
Ethernet HW addr: a4d1d2e366cb on eth2
6 0 1144 0.0 15 0 2338 1.8
Ethernet HW addr: 01005e0000fb on eth2
30 0 5474 3.2 0 0 0 0.0
Ethernet HW addr: 0017c4e3c782 on eth2
237 0 151276 167.6 172 0 42882 12.0
Ethernet HW addr: 001f3a73d7d3 on eth2
710 0 925886 405.6 377 0 17632 8.2
Ethernet HW addr: 001f3b573d59 on eth2
34 0 13979 0.4 72 0 8068 1.6
Ethernet HW addr: ffffffffffff on eth2
56 0 6774 1.4 0 0 0 0.0
Ethernet HW addr: 0022fbabd38e on eth2
87 0 23815 22.8 115 0 40923 44.2
Ethernet HW addr: 00e04c05cb85 on eth2
167 0 159760 3.0 105 0 11715 3.2
32 entries Elapsed time: 0:00 InRate and OutRate are in kbits/sec
Up/Down/PgUp/PgDn-scroll window S-sort X-exit
Figure 5-1: Monitoring Bandwidth with iptraf

5.5.4 Ping Test

To verify connectivity to the Wireless Gateway or to an Access point, an Administrator can send a ping from the WiDirect to the Wireless gateway. Click on ***Tools->Ping*** on the ***Admin*** page and enter the IP address of an access point.

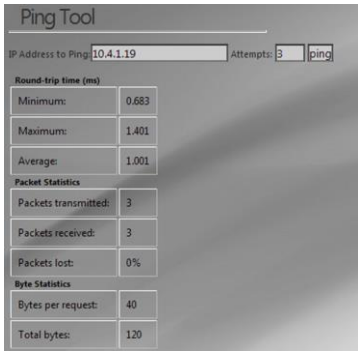


Figure 5-2: Ping Results

5.5.5 DNS Verification

To verify DNS service, use the ***Tools->DNS Query*** tool. Try looking up a public web server such as www.google.com or www.yahoo.com.

5.5.6 Verify APs

Clicking on the ***System Status->Ap Status*** page will provide a list of all the Access Points that are currently monitored by the WiDirect. This page provides a quick way to verify the operation of the Access Points.

Figure 5-2: Access Point Status Page

6 Software

6.1 Software Upgrades & Patching

Upgrades are available on a remote server for customers on an active support contract. To find more details about the upgrades available, please contact the support number for this product.

To activate the upgrade:

1) Perform backup as per instructions in section 4.25.
2) Run "sudo yum update awicp*" from the command line.

6.2 Logs and Log Rotation

Via the ***Systems Configuration*** menu. Administrators can use the ***Log Viewer*** to view and download various system log files. In addition to viewing a static log, the ability to view log files in real-time is enabled by default to assist in network performance monitoring and troubleshooting.

All log files are rotated every night automatically. Each log file can be a maximum of 1 Mb in size and only the last five log rotations are kept.

6.3 Log Location

Most standard logs can be viewed from the ***Admin*** interface menu ***System Configuration -> Logs***. However, if you want more detailed log analysis, SSH to the WiDirect and locate the following log files:

radius	/var/log/radius/radius.log
dhcpd	/var/log/messages
awicp	/root/AWICP/logs/portal.log
awicp-manager	/root/AWICP/logs/manager.log
general syslog	/var/log/messages
nortel messages	/var/log/nortel.log
ftp log	/var/log/xferlog

7 Hardware Diagrams

This section shows the physical port layout of the WiDirect. Figure 7-1 shows the front of the WiDirect

Figure 7-1: Front of WiDirect

The front of the WiDirect consists of a **power** button and a **reset** button.
The LEDs from left to right are **temperature alarm**, **Eth1 network activity**, **Eth0 network activity**, **hard disk activity**, and **Power**.

Figure 7-2 shows the back of the Base WiDirect ACW 50.

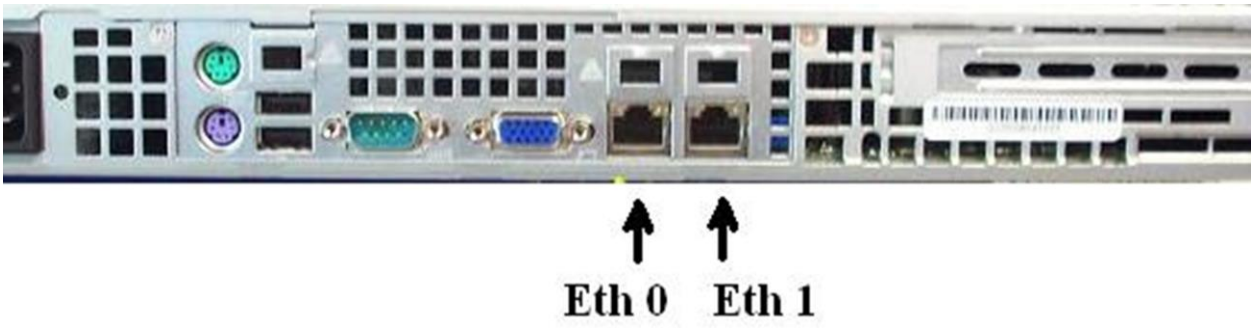


Figure 7-2: Back of the WiDirect

The important ports on the back of the WiDirect are Serial, Eth0, and Eth1. The serial port (green 9 pin) can be used with a null modem cable (38,400 baud) to reach the Command Line prompt.

Eth0 and Eth1 are the network connections on the WiDirect. The Eth0 should be plugged into the Internet side and the Eth1 should be connected to the local side of the network.

Warning: The mouse, keyboard and monitor ports are active and can be used if needed. However, if a keyboard is plugged into the WiDirect, it should not be removed unless the system is first shut down.

Figure 7-3 shows the back of the WiDirect Pro and Figure 7-4 shows the back of the WiDirect Enterprise.

Figure 7-3 Back of the WiDirect Pro

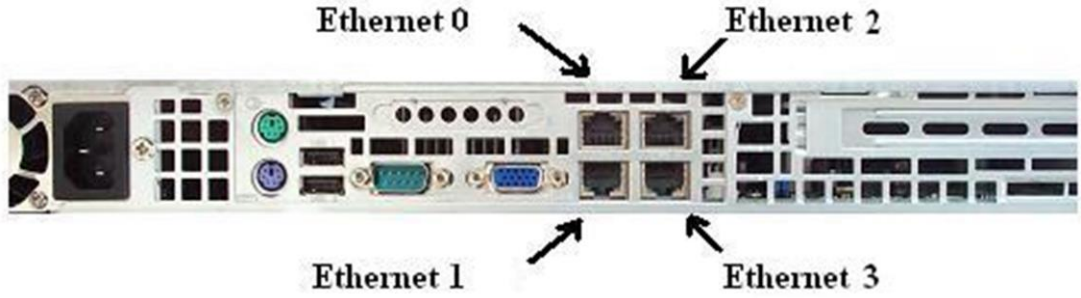


Figure 7-4: Back of the WiDirect Enterprise

The important ports on the back of the WiDirect Pro and Enterprise are Serial, Eth0, Eth1, Eth2 and Eth3. The serial port (green 9 pin) can be used with a null modem cable (38,400 baud) to reach the Command Line prompt.

Eth0 and Eth1 are the network connections on the WiDirect. The Eth0 should be plugged into the Internet side and the Eth1 should be connected to the local side of the network.

Warning: The mouse, keyboard and monitor ports are active and can be used if needed. However, if a keyboard is plugged into the WiDirect, it should not be removed unless the system is first shut down.

Figure 7-5 shows the Front of the WiDirect Micro

Figure 7-5: Front of WiDirect Micro

Figure 7-6 shows the back of the WiDirect Micro:

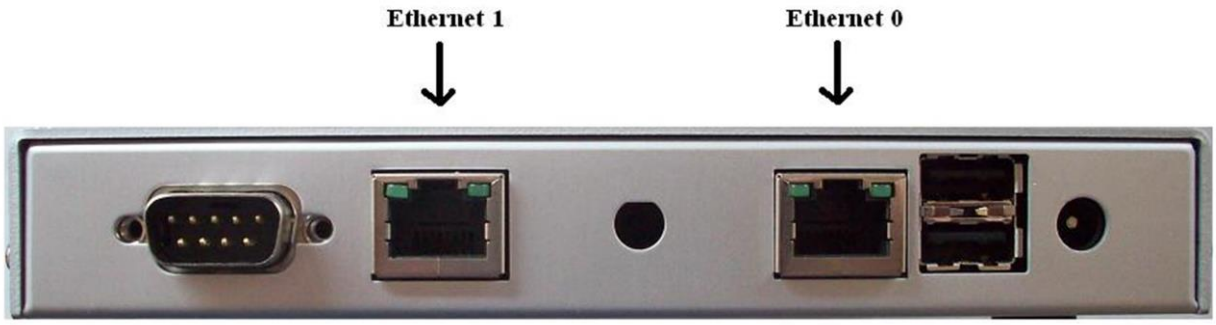


Figure 7-6: Back of WiDirect Micro

The important ports on the back of the WiDirect Micro are Serial, Eth0, and Eth1. The serial port (far left) can be used with a null modem cable (38,400 baud) to reach the Command Line prompt.

Eth0 and Eth1 are the network connections on the WiDirect. The Eth0 port should be plugged into the Internet side and the Eth1 should be connected to the local side of the network.

Figure 7-7 Shows the Back of the WiDirect Carrier:

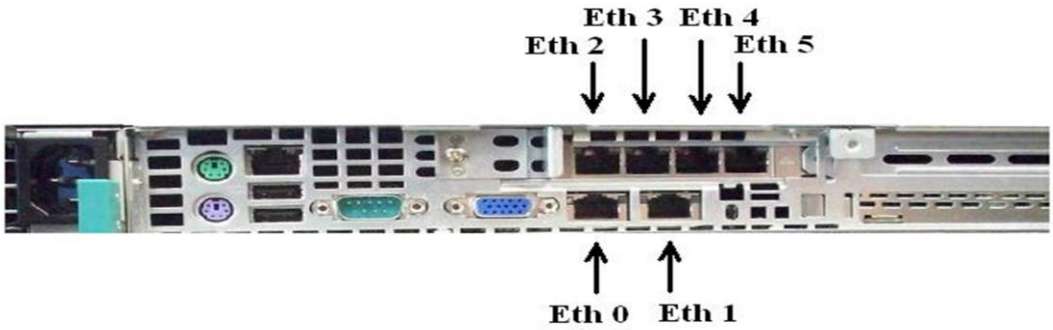


Figure 7-7 Back of WiDirect Carrier

The important ports on the back of the WiDirect Pro and Enterprise are Serial, Eth0, Eth1, Eth2, Eth3, Eth4, Eth5. The serial port (green 9 pin) can be used with a null modem cable (38,400 baud) to reach the Command Line prompt.

Eth0 and Eth1 are the network connections on the WiDirect. The Eth0 port should be plugged into the Internet side and the Eth1 should be connected to the local side of the network.

Warning: The mouse, keyboard and monitor ports are active and can be used if needed. However, if a keyboard is plugged into the WiDirect, it should not be removed unless the system is first shut down.

8 Technical Support

Support Contact Details

Dedicated Phone Support:	(443) 294-0000
Dedicated e-mail support:	support@allcitywireless.com
Self-support:	www.allcitywireless.com/support
Corporate Address:	326 First Street Suite 23 Annapolis, MD 21403